2

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A FRAMEWORK FOR AN INTEGRATED DEFENSE
COMMUNICATION NETWORK FOR THE
REPUBLIC OF CHINA ARMED FORCES

by

Wang Yu-Lin

March 1991

Thesis Advisor: Judith H. Lind

Approved for public release; distribution is unlimited

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE					Form Approved OMB No 0704-0188
1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b RESTRICTIVE MARKINGS			
2a SECURITY CLASSIFICATION AUTHORITY		3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited			
2b DECLASSIFICATION/DOWNGRADING SCHEDULE					
4 PERFORMING ORGANIZATION REPORT NUMBER(S)		5 MONITORING ORGANIZATION REPORT NUMBER(S)			
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) AS	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School			
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000			
8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER			
8c ADDRESS (City, State, and ZIP Code)		10 SOURCE OF FUNDING NUMBERS			
		PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification) A FRAMEWORK FOR AN INTEGRATED DEFENSE COMMUNICATION NETWORK FOR THE REPUBLIC OF CHINA ARMED FORCES

12 PERSONAL AUTHOR(S)
WANG Yu-Lin

13a TYPE OF REPORT Master's Thesis	13b TIME COVERED FROM ______ TO ______	14 DATE OF REPORT (Year, Month, Day) 1991 March	15 PAGE COUNT 88

16 SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Network Communication Technologies;Defense Data Network (DDN);Integrated Services Digital Network (ISDN)

19 ABSTRACT (Continue on reverse if necessary and identify by block number) This thesis discusses communication systems currently in use by the Republic of China (R.O.C.) Armed Forces and explores ways that the R.O.C. may increase the capability of its national defense by improving current communication networks. Modern network communication and components techniques such as digital data transmission, network protocols, network topologies, switching technologies, and transmission media are discussed. The U.S. Defense Data Network (DDN) is used as a model for a successful military network. The DDN technology and Integrated Services Digital Network (ISDN) standards are combined with concepts from modern communication technologies to develop the conceptual framework for a proposed Integrated Defense Communication Network (IDCN) for the R.O.C. Armed Forces. This framework is intended for use by the R.O.C. Department of Defense in establishing a nation-wide communication system that will improve its administration management, logistic supply, intelligence collection, and auxiliary tactical communication capabilities.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a NAME OF RESPONSIBLE INDIVIDUAL LIND, Judith H.	22b TELEPHONE (Include Area Code) 408-646-2543	22c OFFICE SYMBOL OR/Li

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603

UNCLASSIFIED

Approved for public release; distribution is unlimited

A Framework for an Integrated Defense Communication Network for the Republic of China Armed Forces

by

Yu-Lin Wang
Lieutenant Commander, Republic of China Navy
B.S. Republic of China Naval Academy, 1979

submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE
IN TELECOMMUNICATION SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1991

Author: Yu Lin WANG
Yu-Lin Wang

Approved by: Judith H Lind
Judith H. Lind, Thesis Advisor

Dan C Boger
Dan C. Boger, Second Reader

S.L. Mehay, Acting Chair
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis discusses communication systems currently in use by the Republic of China (R.O.C.) Armed Forces and explores ways that the R.O.C. may increase the capability of its national defense by improving current communication networks. Modern network communication and components techniques such as digital data transmission, network protocols, network topologies, switching technologies, and transmission media are discussed. The U.S. Defense Data Network (DDN) is used as a model for a successful military network. The DDN technology and Integrated Services Digital Network (ISDN) standards are combined with concepts from modern communication technologies to develop the conceptual framework for a proposed Integrated Defense Communication Network (IDCN) for the R.O.C. Armed Forces. This framework is intended for use by the R.O.C. Department of Defense in establishing a nation-wide communication system that will improve its administration management, logistic supply, intelligence collection, and auxiliary tactical communication capabilities.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ASCII	American Standard Code for Information Interchange
ADP	Automated data processing
ARPANET	Advanced Research Projects Administration Network
AUTODIN	Automated Digital Network
C3-I	Command, control, communication, and intelligence
CCITT	International Telegraph and Telephone Consultative Committee
CSN	Circuit Switching Node
DCA	Defense Communications Agency
DCS	Defense Communications System
DDN	Defense Data Network
DISNET	Defense Integrated Secure Network
FDDI	Fiber Distributed Data Interface
FDM	Frequency-Division Multiplexing
FPS	Fast Packet switching
FTP	File Transfer Protocol
IDN	Integrated digital network
IDCN	Integrated Defense Communication Network
ISDN	Integrated Services Digital Network
IST	Inter-switch trunks
JCS	Joint Chiefs of Staffs
LAN	Local Area Networks
MAN	Metropolitan Area Networks

MILNET	Military network
MIS	Management information system
NAC	Network access component
NCS	National Communications System
OSI	Open Systems Interconnection reference model.
PBX	Private Branch Exchange
P.R.C.	People's Republic of China
PSN	Packet switching node
R.O.C.	Republic of China
SACDIN	Strategic Air Command Digital Information Network
SCINET	Secure Compartmented Information Network
STDM	Statistical Time-Division Multiplexing
TDM	Time-Division Multiplexing
UHF	Ultra High Frequency
VHF	Very High Frequency
WAN	Wide Area Networks
WINCS	Intercomputer Network Communication Subsystem

I. INTRODUCTION

A. THE REPUBLIC OF CHINA AND THE PEOPLE'S REPUBLIC OF CHINA

Since 1949, China has been a divided country similar to Korea. At that time the government of the Republic of China (R.O.C.) moved its seat from the mainland to the island of Taiwan, due to a military takeover by Chinese Communists. Since then the R.O.C. government has found it necessary to protect itself against the Communist threat. This situation has existed for 40 years on this small democratic island.

The two Chinese governments are independent and hold opposite political views. The Peoples Republic of China (P.R.C.) controls most of the geographical territory, mainland China, and one billion people. Both the R.O.C. and the P.R.C. insist that they represent "China." The rest of the world currently recognizes both governments, based on formal diplomatic relationships.

Each of the two governments has as its goal to reunite Taiwan and mainland China under its system. The P.R.C. has declared that it will never give up the struggle to "liberate" Taiwan and include it under the Communist system [Ref. 1:p. 202]. Thus the R.O.C. must maintain strong military forces to ensure its national security and avoid Communist takeover.

The R.O.C. consists of the several islands that make up Taiwan, along with the Taiwan Strait. Total population is approximately 20 million people. Taiwan is located in the western Pacific area, approximately 80 miles from the mainland. Its location requires that the R.O.C. control the sea lanes between the East and South China Seas, to ensure the country's continued freedom (as shown in Figure 1-1) [Ref. 2:p. 883]. Politically the government is a demccracy, unlike the Communist-governed mainland.

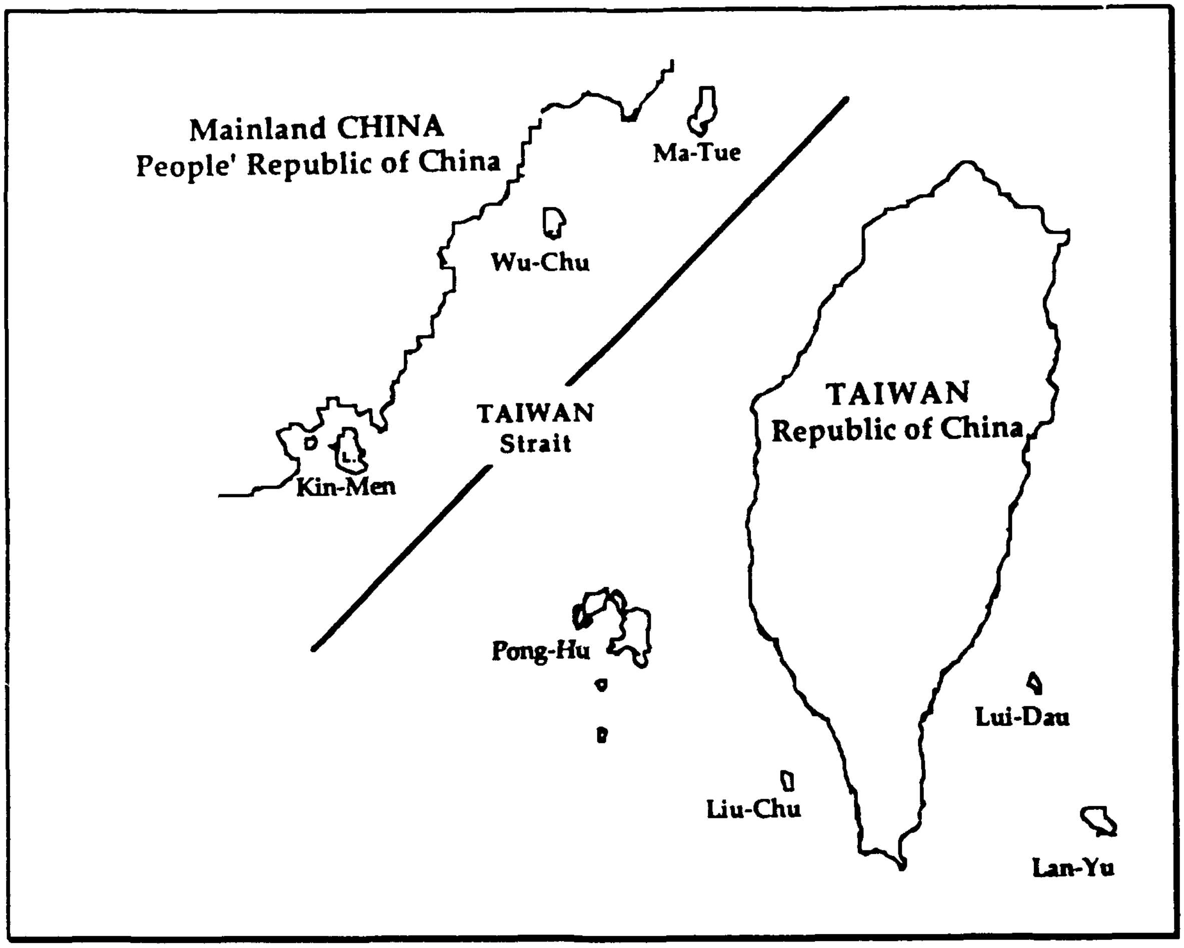

Figure 1-1. The Republic of China, Taiwan.

B. NATIONAL DEFENSE FOR THE R.O.C.

1. ROC Armed Forces

The R.O.C. has developed and maintained modern armed forces for its defense. In this way it has ensured its ability to continue to resist mainland

China's aggression. At the same time, R.O.C. strength has helped maintain the security of the western Pacific area.

The objective of the armed forces on Taiwan is to guarantee the nation's sovereignty and independence. The military also must prepare to return to the mainland if the opportunity arises. Strong military forces also protect the country from P.R.C. ambitions, and thus protect the national security. To be effective, it is necessary that the R.O.C. control the oceans and air space around the island. Modern military equipment is critical in order to maintain the country's defensive capability.

The R.O.C. Armed Forces are organized along the usual world lines into an Army, Navy, and Air Force structure, as shown in Figure 1-2 [Ref. 1:p. 203]. Total armed forces number approximately 464,000. This includes 310,000 in the Army, 77,000 in the Navy (including 39,000 in the Marine Corps), and 77,000 in the Air Force [Ref. 2:p. 517]. The R.O.C. military's size and state of training make it one of the most formidable in Asia. However, the P.R.C. forces are much greater in size. Comparison of the size of the R.O.C. forces with those of the P.R.C. is shown in Table 1-1. [Ref. 2:p. 119]

2. Current Defense Environment

R.O.C. political relations with the U.S. have been cool since 1972 when the U.S. stated its intention to phase out its forces in the R.O.C. The U.S. interest in normalizing relations with the P.R.C. has resulted in further deterioration of the relationship.

The R.O.C., fearing a potential end to the U.S. defense equipment supply, is pressing its defense industries to boost their capabilities and output.

The government is also increasing its research and development efforts in the defense electronics field. [Ref. 1:p. 202]

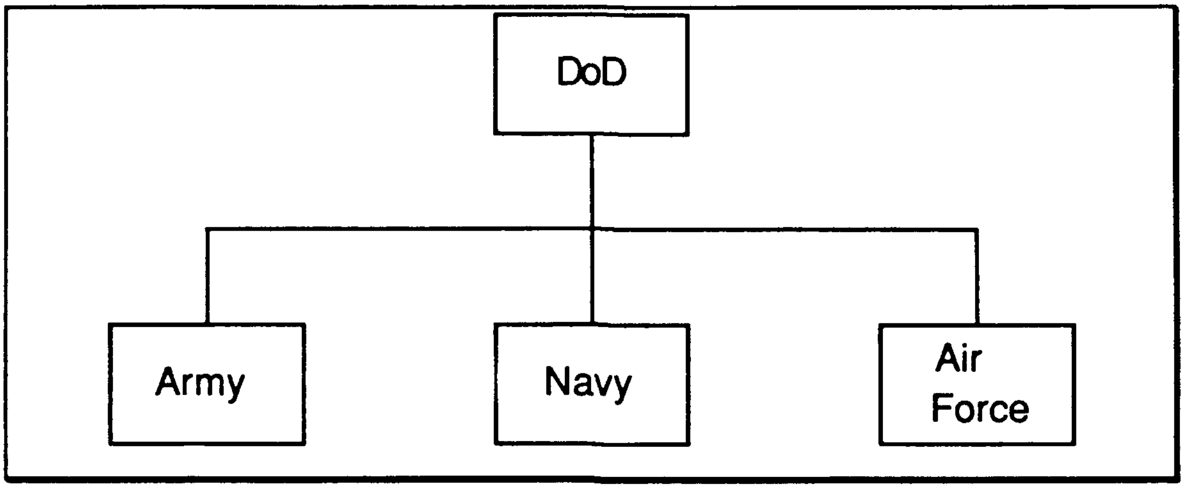

Figure 1-2. R.O.C. Military Structure

TABLE 1-1 COMPARISONS OF THE R.O.C. AND P.R.C. MILITARY FORCES

	ARMY	NAVY	AIR FORCE	TOTAL MILITARY
R.O.C. Taiwan	310,000	77,000	77,000	464,000
P.R.C.	3,160,000	350,000	490,000	4,000,000

One of the R.O.C.'s major concerns is the loss of world diplomatic recognition and accompanying closure of defense markets, particularly in Europe. Under P.R.C. pressure, in 1983 the Swiss government cancelled a contract for repair of armored vehicles by R.O.C. corporations. In 1984, the Netherlands turned down a R.O.C. request for four additional submarines of the Walrus type that had been ordered in 1981. [Ref. 1:p. 204]

Several efforts at defense self-sufficiency have resulted from these concerns, including the establishment of new Weapons Institutions for research into replacement sources for U.S. arms. The Chung Shan Institute of Science and Technology, the research agency of the R.O.C. government, is tasked with developmen' ᶠ critically needed defense equipment. [Ref. 1:p. 204]

C. MILITARY COMMUNICATIONS

It is critical that the R.O.C. Armed Forces have an efficient communication system network to support command, control, communication, and intelligence (C3I), administration management, logistics supply, and auxiliary tactical communication systems. Such a modern communication system network is vital for operational capability.

Currently, communications in the R.O.C. Armed Forces are carried out using communications technologies such as computers, facsimile transmission, telephones, radio, telex, and air and surface mail. Each branch of the military has a separate communication system, but all have the same objective: to conduct the mission.

Military communications must be rapid, secure, reliable and flexible. The current R.O.C. Armed Forces communications systems fall short in several of these areas.

1. Speed

Current military communication systems are not interconnected among the branches of the armed forces. Messages between the services and between various bases within each of the services must be sent using traditional techniques, such as radio transmission, facsimile transmission, telephone, or mail. These communication techniques require unnecessary time and manpower.

2. Security

Most current R.O.C. military communication systems are used with traditional security measures (such as coding, cipher, etc.) for radio, telephone, and mail messages. If a message is intercepted, coded and cipher messages can be decoded and deciphered with relative ease.

3. Reliability

Most current world radio communications systems are affected by weather, background noise, and jamming, decreasing the reliability of such systems. This is the case with the R.O.C. Armed Forces.

4. Flexibility

Existing communication devices (radios, telephones, etc.) are not interoperable. Thus only one communication medium can be used for each message, no matter how it must travel. Current transmission lines and routes are fixed, rather than flexible.

D. TELECOMMUNICATION AND NETWORKS FOR NATIONAL DEFENSE

The field of telecommunications has undergone significant changes in the past two decades. Rapid development of new computer and communications technologies has had a great influence on both national defense and economics. This is especially true in the area of military communication. Requirements to manage defense resources and conduct C3I operations now demand rapid and dependable communications.

American Telephone and Telegraph Corporation introduced the first commercial digital carrier system in the United States in the early 1960s [Ref. 3:p. 3]. This technology was introduced to most other countries soon thereafter. Between 1970 and the present time, the fields of voice (analog) communications and data (digital) communications largely have merged, to result in the field of telecommunications.

Telecommunications use various electrical and electromagnetic media that permit transmission of large amounts of data over great distances at high speeds. Telephones, telegraph, radio and microwave transmissions, television, and satellites all are used for telecommunication. When two or more communication devices are linked together, the result is a network that may be used to share information and other resources. Telecommunications permit such resource sharing over great distances, thereby enabling the expansion of networks to a very large scale.

Information related to command and control must be transmitted rapidly and accurately in order to conduct military operations and thus can benefit from telecommunications networks. In addition, administration, management, logistics, and office automation all can be enhanced by using telecommunication networks to improve data processing and transmission.

Networks and the equipment to operate them are very important to modern military communications. Through the use of such technology, large amounts of information can be transmitted accurately and effectively.

A Defense Data Network (DDN) has been used by the U.S. military forces for communication for more than ten years [Ref. 4:p. 121]. This system provides a major channel for much U.S. military and government communication. DDN experience has demonstrated that this technology meets many of the demands of modern military communications. The network has shown that such technology can result in significant cost saving, interoperability, system survivability, and reliability.

As the R.O.C. Armed Forces seek ways to modernize their communications systems, the U.S. DDN can serve as a model. Combining DDN technologies with other modern communication technologies, it should be possible to define a Integrated Defense Communication Network (IDCN) that would be appropriate and attainable for the R.O.C. military.

E. GOALS AND OBJECTIVES OF THIS STUDY

This study discusses communication systems currently in use by the R.O.C. Armed Forces and explores ways that the R.O.C. may increase the capability of its national defense by improving current communication networks. The U.S. DDN is used as a model for a successful military network. The U.S. DDN model is combined with concepts from modern communication technologies to develop the conceptual framework for a proposed Integrated Defense Communication Network (IDCN) for the R.O.C. Armed Forces. This framework is intended for use by the R.O.C. DoD in improving its administration management, logistic supply, intelligence, and auxiliary tactical communication capability. In order to achieve these goals, the following objectives have been met.

- A search of the current literature, including periodicals, technical journals, and books, was conducted.
- The roles and responsibilities of the R.O.C. DoD and Armed Forces were reviewed.

- Modern network communication and components techniques such as network architecture, transmission media, and switching technologies were explored.
- The U.S. DDN system was studied to trace its evolution, and Integrated Services Digital Network (ISDN) technologies were evaluated for their applicability to the R.O.C. military.
- U.S. DDN, ISDN, and modern integrated digital communication technologies were used to develop a framework for a proposed IDCN, based on the unique requirements of the R.O.C. Armed Forces.

F. SCOPE

Emphasis of this thesis is on development of a framework for a possible IDCN, based on U.S. DDN and ISDN concepts and technologies, as well as other modern communication technologies. This thesis does not propose to make specific, detailed recommendations for how the IDCN might be constructed for the R.O.C. Armed Forces. Rather, the goal is to make use of the successful U.S. DDN and other new communication technologies to lay the groundwork for an IDCN for the R.O.C.

The first chapter of this study provides a brief introduction to the R.O.C. and its current situation, national defense policy, military organization, and communication problems. Telecommunication technology also is described briefly. Chapter II examines in detail digital data communication technologies, network technologies, and network components. Chapter III presents a overview of the U.S. DDN and how it has been used by the U.S. military. It also describes the services and examines the benefits of this network. Chapter IV presents an overview of ISDN concepts, reviews the evolution of ISDN, and examines the technologies, services, and benefits of ISDN. Chapter V proposes a way that existing technologies may be used to develop an IDCN for the R.O.C. Armed Forces. This final chapter provides conclusions based on this study and recommends how the framework proposed here might be implemented for the R.O.C. Armed Forces.

II. NETWORK COMMUNICATION TECHNOLOGIES

A. DIGITAL DATA COMMUNICATIONS AND TECHNOLOGIES

Various kinds of signals are transmitted in modern integrated communication networks. These include audio, video, and both digital and analog data signals. Several techniques have significant effects on the quality of data communications. These techniques include data encoding, transmission, compression, and multiplexing.

Data encoding is the process whereby a code is used to represent individual characters or groups of characters in a message, as needed to optimize data transfer via various transmission media. The process of encoding is referred to as modulation, and involves transferring source data onto a carrier signal with a specific frequency. Demodulation returns the signal to its original form after transmission.

Signal transmission media are categorized either as guided or unguided, depending on the basic technique used to link stations of a communication network. Data compression and multiplexing have been developed to make the best use of transmission equipment.

1. Data Encoding

A basic consideration for all digital data communications systems is that each of the possible data characters being transmitted must be assigned a unique code that is compatible with the transmission medium. A means must be provided at the data source for converting each character to its associated transmission code (usually equivalent to a sequence of zeros and ones), and a similar means must be provided at the destination for converting the code back to its proper character. [Ref. 4:p. 67]

Communications networks can carry digital data or signals (such as computer communication) and also analog data or signals (such as telephone communications). Prior to transmission, each of these data types may have to be encoded in order to be compatible with the network transmission medium. Digital-to-digital coding converts digital signals to another form of digital signal in order to use a more efficient encoding structure. Digital-to-analog coding converts the original digital signals to analog signals in order to use analog transmission facilities. Analog-to-digital coding represents analog voice and video signals as digital signals in order to use more efficient, less expensive, and less complex equipment, and to provide digital technology for all forms of transmission. Analog-to-analog coding converts analog voice signals from one frequency to a different portion of the analog frequency spectrum and higher bandwidth, in order to take advantage of the capacity of higher bandwidths. [Ref. 5:p. 65]

The encoding process most widely used for modern digital data communications systems is the American Standard Code for Information Interchange (ASCII). The ASCII code uses a unique sequence of seven ones and zeros (each referred to as a bit) to present each of 128 different characters. This system can be used to encode the alphabet letters, numerals, punctuation marks, and a number of special characters used in data communication.

Other bits are usually present in each coded character. A parity check bit may be added as a means of detecting a transmission error. For asynchronous transmission, it is necessary to add additional start and stop bits. The entire coded character, consisting of seven to ten bits, is referred to as a frame. An example of ASCII encoding for the letter W is shown as Figure 2-1 [Ref. 6:p. 339].

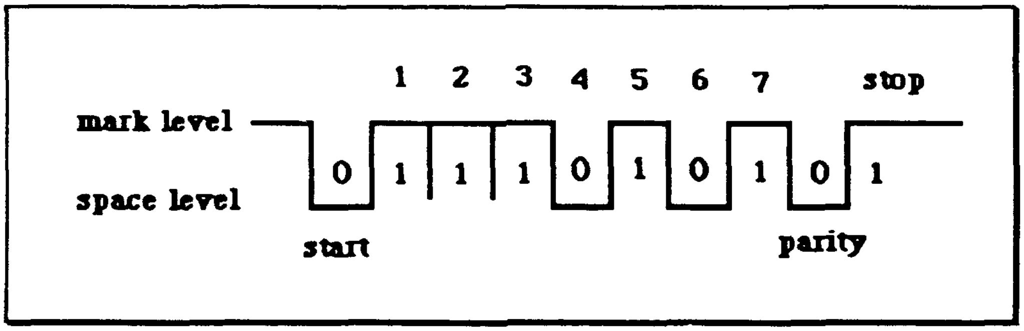

Figure 2-1. Asynchronous Encoding of the Letter W in ASCII Form

2. Data Compression

Most data communication techniques transmit characters that have been coded as a constant, fixed number of bits. Fixed length codes were developed because computers require a constant number of bits per character to process data efficiently. However, some characters, such as the question mark and period, do not require the full seven bits for adequate representation. To increase the data transmission rate, it is possible to use a variable-length code. This is referred to as data compression. The technique of data compression results in communications that are less expensive, less subject to errors, and with smaller data volumes. [Ref. 5:p. 197]

3. Data Transmission

Data transmission is the process whereby a signal travels between a transmitter and a receiver. The successful transmission of data depends principally on the quality of the signal being transmitted and the characteristics of the transmission medium. Due to signal distortion or transmission impairments, the signals that are received may be different from those transmitted. Distortions primarily are determined by the nature of the transmission medium used. [Ref. 4:p. 46]

Two generic approaches are used for signal transmission, referred to as guided and unguided transmission techniques. Guided transmission media include wires, coaxial cable, and optical fibers. Unguided transmission media make use of the electromagnetic spectrum and its properties in free space.

Both analog and digital data signals may be transmitted using either guided or unguided transmission techniques. Analog transmission sends signals without regard to their content; the signals may represent analog data or digital data. Digital signal transmission works only with digitized signals.

Both analog and digital signals become weaker after traveling a certain distance. Both transmission techniques require either an amplifier to boost the signal strength or a repeater to retransmit the signal.

4. Multiplexing

Multiplexing allows greater use of transmission equipment without compression of the data. The term refers to a variety of techniques used to make more efficient use of a transmission facility by allowing it to transfer data between several devices at the same time, that is, by multiplexing a number of signals onto the same medium, sometimes referred to as a mux bus. Lower-speed voice or data signals are accepted from source equipment and combined into one high-speed stream for transmission to their destinations. The basic functional diagram for multiplexing is shown in Figure 2-2. [Ref. 4:p. 166]

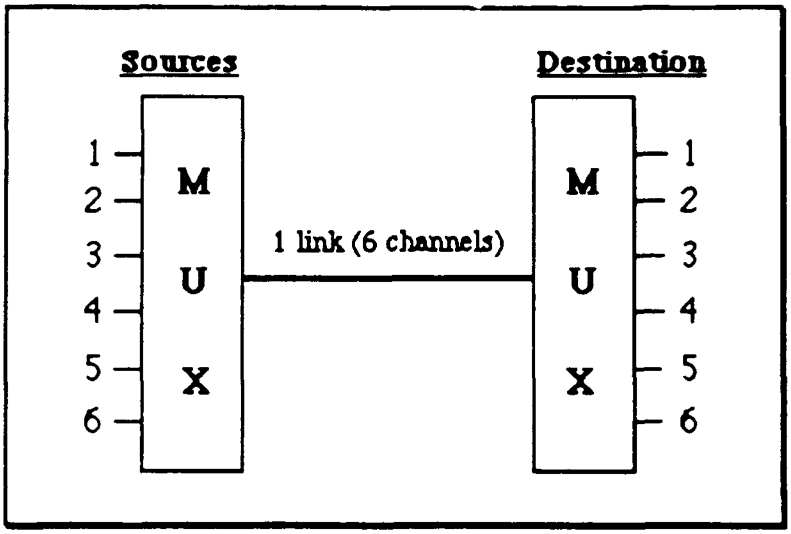

Figure 2-2. Basic Multiplexing Technique

One common multiplexing technique is frequency-division multiplexing (FDM). Each source signal is modulated onto a different carrier frequency. The carrier frequencies are sufficiently separated so that the bandwidths of the signals do not overlap, as is shown as Figure 2-3.

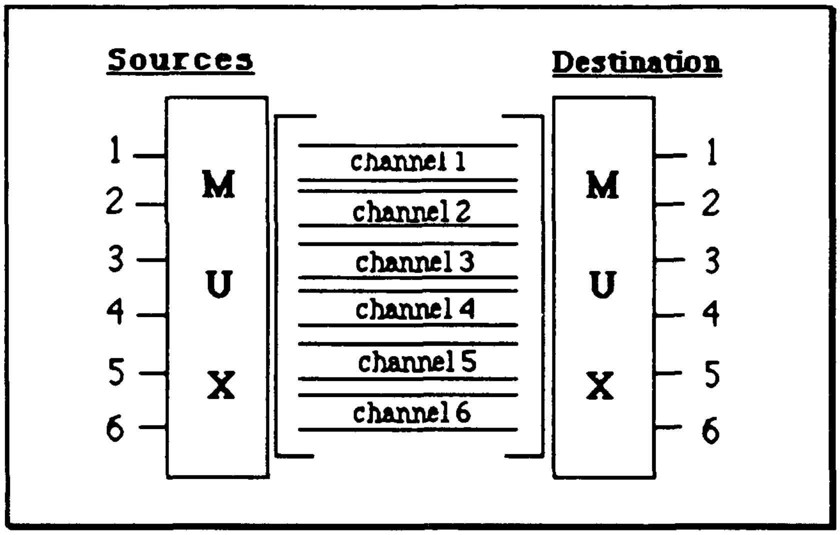

Figure 2-3. Frequency-Division Multiplexing Technique

Time-division multiplexing (TDM) is also referred to as synchronous multiplexing. A single transmission path carries several digital signals at the same time by interleaving very small portions of each signal in time, as shown as Figure 2-4.

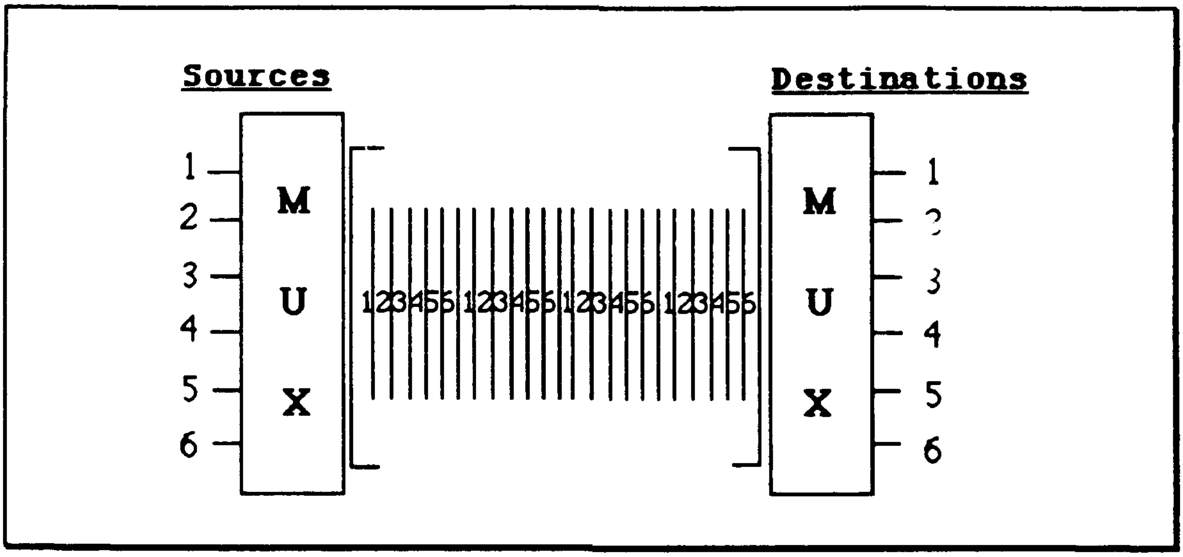

Figure 2-4. *Time-Division Multiplexing Technique*

Statistical time-division multiplexing (STDM) allows the use of a number of input/output lines at one end of the transmission and a higher-speed multiplexed line at the other. Each input/output line has a buffer associated with it. For transmission input, the source input buffers are scanned and data are collected until a frame is filled, at which time the frame is sent. The destination multiplexer receives the frame and distributes the slots of data to the appropriate output buffers. The STDM process provides same function as TDM techniques, but is more efficient in its use of transmission channels, as is shown as Figure 2-5. [Ref. 4:p. 174]

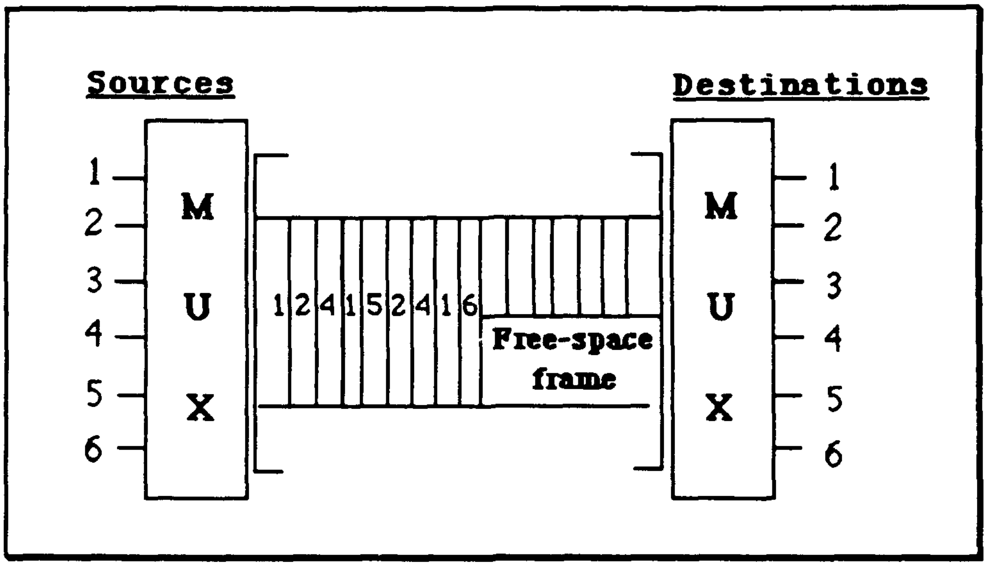

Figure 2-5. Statistical Time-Division Multiplexing Technique

B. NETWORK TECHNOLOGIES

The basic functions of a computer communication network are to make it possible for geographically remote end users to communicate and to provide time-sharing and resource-sharing for both groups and individual users. A communication network can be defined as an interconnected system of transmission lines and other equipment that provide communication, with multiple connections between destinations and sources, each remote from the others, exchanging data as necessary to perform specific functions. [Ref. 7:p. 685]

The incorporation and inclusion of computers in network communication has had a major impact on networks. Communications applications, among both humans and machines, have flourished with the addition of the computer as a tool, resulting in lower costs and higher reliability.

Networks generally are categorized as local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). Network components include a variety of switching equipment, transmission media, security devices, and user equipment. Establishing a communications path among various remote users and kinds of equipment has been made possible through use of a standard layered network architecture called the Open Systems Interconnection (OSI) reference model. [Ref. 8:p. 4]

1. Network Protocols

Communication among data processing devices such as computers is much more complex than voice communication. Communication among computers and other equipment from various vendors and for different models from same vendor requires that data processing devices implement a set of communications functions that will allow them to perform tasks cooperatively. This set of functions is organized into a network communications architecture. Most typically, network architectures follow a layered hierarchical model. [Ref. 4:p. 376]

The International Organization for Standardization in 1977 established a subcommittee to develop such an architecture. The result is the OSI reference model, adopted in 1983. The OSI partitions communication devices into a set of layers: physical, data link, network, transport, session, presentation, and application, as shown in Figure 2-6. Devices in each layer perform a related subset of the functions required to the communicate with another system. The OSI model provides the basis for connecting various "open" or nonuniform systems for distributed applications processing. [Ref. 5:p. 270]

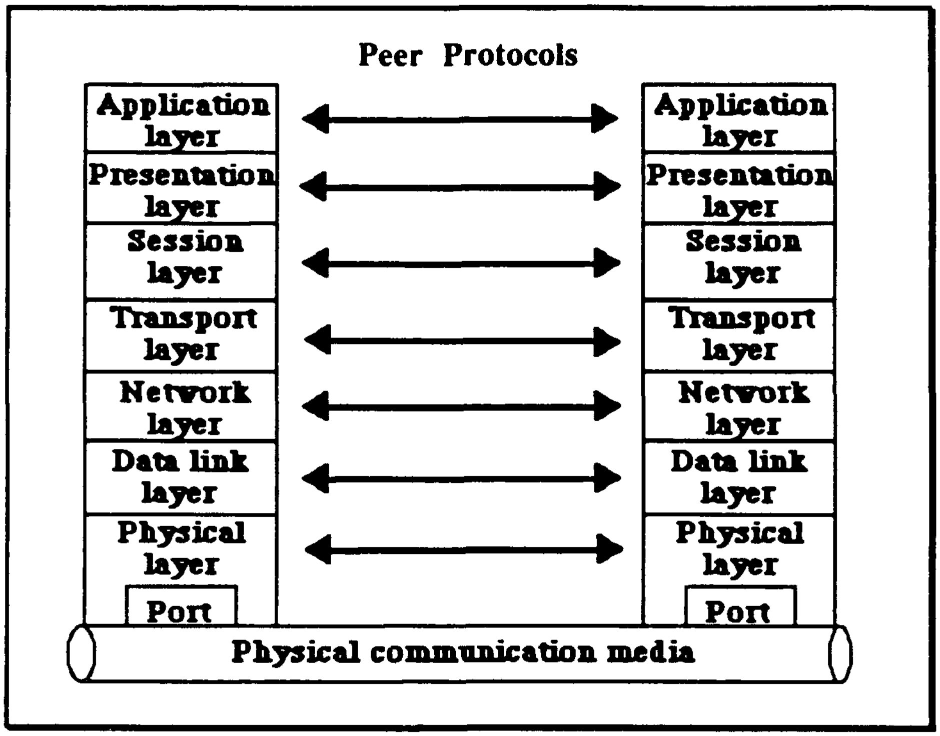

Figure 2-6. The Open System Interconnection Reference Model

The function of the OSI physical layer is to provide a physical connection between the end users and to transmit raw bits of data across the physical transmission resources. The data link layer provides the capability for error detection and control between machines, to achieve efficient utilization of resources. The network layer provides routing functions to control the transportation of data from source-host to destination-host. The transportation layer provides reliable, transparent transfer of data between end points, and also provides end-to-end error recovery and flow control. The session layer provides the control structure for communication between applications. The presentation layer enables the application processes to work independently, even through there are differences in data representation. The application layer provides access to the OSI environment for users and also provides distributed information services. [Ref. 3:p. 75]

The OSI provides a common basis for the development of new systems interconnection standards and devices, while placing existing standards in perspective within the overall reference model. The exchange of information among various systems is made possible through their mutual use of the applicable standards. International teams of experts also may work productively and independently on the development of equipment and standards tor the functions represented by each layer of the OSI.

2. Network Topologies

Network topology and the transmission medium are the two characteristics that determine the types of data that can be transmitted on a given network. These characteristics also determine the speed and efficiency of communications, and the kinds of applications that the network may support.

Topology refers to the architecture or structure used to link the terminals and nodes of a network. Four kinds of topology are common, as shown in Figure 2-7. [Ref. 4:p. 332]

a. Star

Star topology uses a central switching element to connect all the nodes in the network. A dedicated path is established between two stations when they wish to communicate.

b. Ring

Ring topology consists of a closed loop o^f^ nodes. Circulated data tradeoff is provided around the ring along a series of point-to-point data links. Each station must wait to transmit until its next turn in the cycle, resulting in transmission delay times that are a function of ring size and transmission speeds.

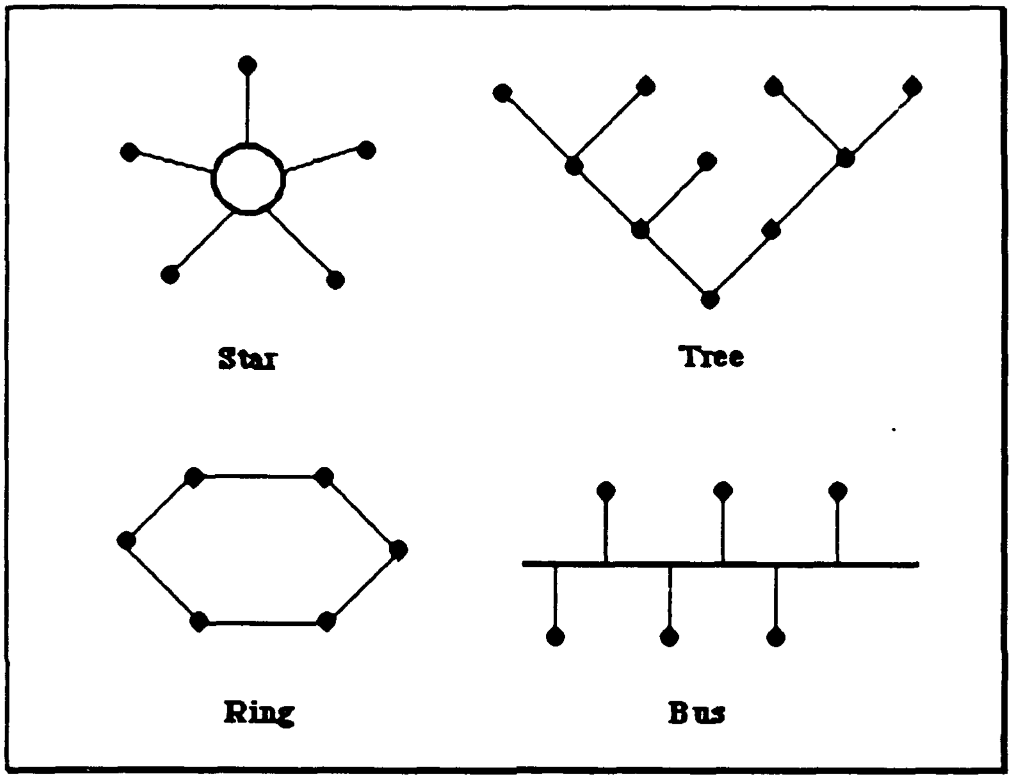

Figure 2-7. Common Network Topologies

c. Tree

Tree topology is characterized by the use of a multipoint medium. That is, nodes are arranged in a pattern similar to a tree, with one or more trunks and several branches. All users are connected to the single transmission medium via simple passive taps. Only one user can transmit at a time, using tree topology.

d. Bus

Bus topology is the most basic type of tree, containing only one trunk with no branches. Since all devices share a common communications medium, only one pair can communicate at a time. Bus systems are ideal for short distance network communication within a single building, connecting a large number of devices that require intercommunication capability. [Ref. 4:p. 333]

3. Basic Types of Networks

Netw.:ks can be divided into three categories, based on the size of the areas they cover. These are LANs, MANs, and WANs. The three types may be interconnected, as is shown as Figure 2-8. [Ref. 9:p. 24]

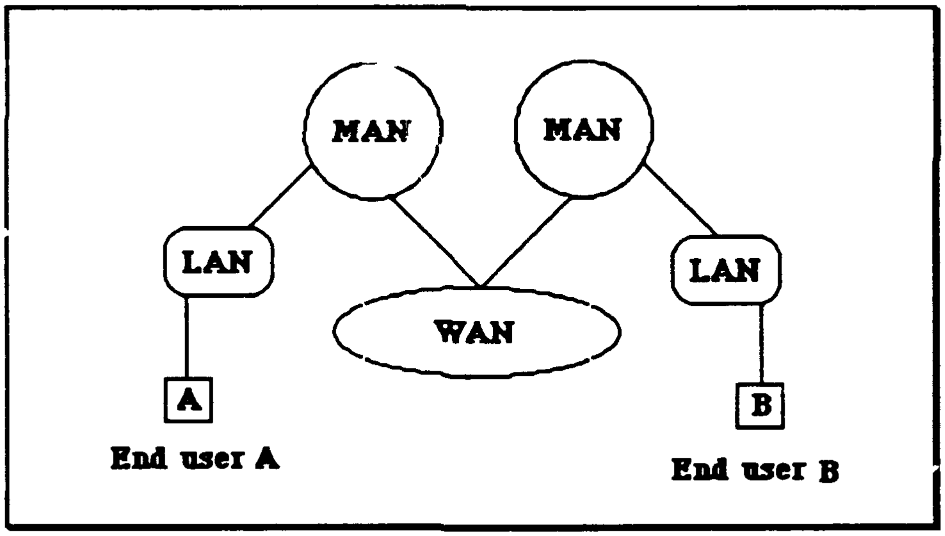

Figure 2-8. Interconnection of Local, Metropolitan, and Wide Area Networks

a. Local Area Network

LANs are designed to allow computers using common protocols to communicate at very high bit rates over a small geographical area. Both military and civilian orgənizations use LANs to increase employee productivity and efficiency and to permit several computers and users to share expensive hardware such as high-speed printers and disk units. LAN equipment typically is owned by the organization using the facility.

LANs connect user devices that are located in relatively close proximity to one another, usually in an area between a few hundred square meters and several thousand square meters. Data, voice signals, and images can be transmitted between user stations and computers. The transmission rate of a LAN ranges from 1 Mbps to 20 Mbps, higher data rates than usually are possible with networks covering larger areas. Error rates also are considerably better. [Ref. 10:p. 25]

b. *Metropolitan Area Network*

MANs typically cover a larger geographical area than does a LAN. As the name implies, computers throughout a city (or similar area up to 60 miles in diameter) can be linked via a MAN. LAN technology generally is used, including protocols, digital technologies, and topologies. Functionally, a MAN usually is used to link several LANs in order to form one large single network where all users can communicate with each other. In some cases a MAN and its component LANs may by logically separate, but are located in the same physical facility. [Ref. 10:p. 25]

c. *Wide Area Network*

WANs also are called long haul networks. They are designed to provide transmission paths between various individual computers, LANs, and MANs to form a communication network. WANs are used to transmit a variety of signals, including data, voice, and images. WANs may use different transmission media and protocols than LANs, and, as a result, may have relatively lower reliability. [Ref. 10:p. 25]

The increasing importance of digital data communication has resulted in great growth and improvement in WANs. The technology needed to support both voice and data communication continues to improve, and new technologies are rapidly applied to maximize the performance of WANs.

C. NETWORK COMPONENTS TECHNOLOGIES

The components that make up a network determine its characteristics. These components include devices that connect users to the network, that route the transmitted signals, and that carry the signals along the designated path. Several important technologies are related to these components. They include switching technologies and transmission media technologies.

1. Network Switching Technologies

The process of entering data into a network, routing it to its destination, and controlling it during transmission is referred to as switching. That is, switching technology provides the network connections. Three switching techniques are common; these are referred to as circuit switching, message switching, packet switching, and fast packet switching. These technologies enable end users to communicate with each other via data, voice, and images.

a. Circuit Switching Technologies

Circuit switching technology is used for telephone communication networks to transmit both data and voice signals. Circuit switching provides a transparent, relatively inexpensive, and highly reliable form of transmission service. Circuit switching technology development primarily has been driven by the requirements of handling large quantities of voice traffic. This technology provides a dedicated communication path link through circuit switching nodes (CSNs) between two end users, with other users provided pathways in sequence. A typical generic circuit switching network is shown as Figure 2-9. [Ref. 11:p. 20]

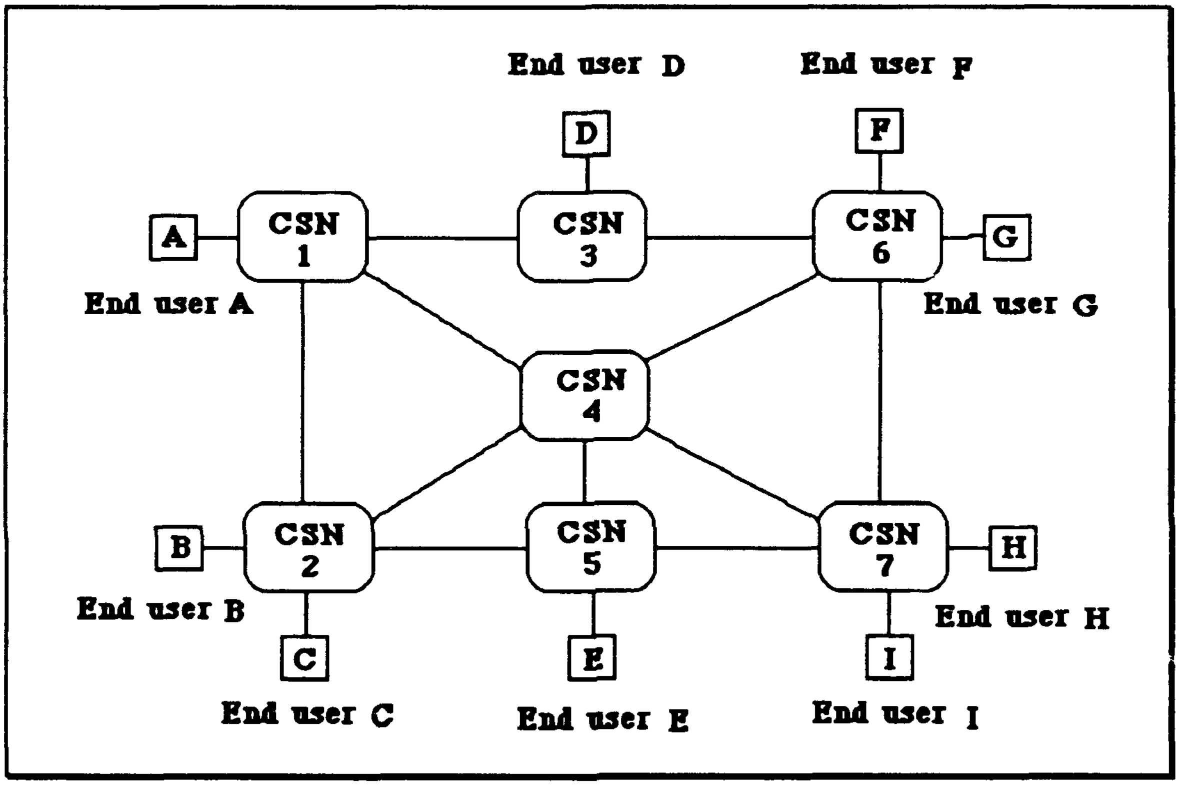

Figure 2-9. Generic Circuit Switching Network

For the circuit switching process, an end-to-end circuit first must be established before data can transmitted. Time is required to set up the communication path between the two users. If many users try to communicate simultaneously, some may get "busy signals" due to lack of internal switching or trunk capacity.

Once the path has been established, the only data transfer delay is the propagation time for the electromagnetic signal. As a consequence of the established path, there is no danger of congestion. This is an efficient type of circuit for voice communication, since communications are transmitted with minimal delay. Both digital and analog signals can transmitted through this kind of circuit. Generally the link between end users is full duplex, that is, data may be transmitted in both directions.

When communication has been completed the circuit is disconnected. This is accomplished through a "terminated" signal from one of the two end destinations initiated by an action such as hanging up the phone. The "terminated" signal frees the communication path that had been established by deallocating those nodes that had been involved in the communication.

Since circuit switching technology provides full duplex connections between end users, it is relatively inefficient. Even if no data or voice signals are being transmitted, the dedicated path is occupied continuously. Multiplexing technology thus is used to increase the utilization of each communication channel. [Ref. 11:p. 22]

(1) Signal Routing. The basic function of routing is to define a path through a number of trunks and switching nodes from the end user placing the call to the call's recipient. Establishment of the signal route is very important in a large circuit switching network. The two end users usually are far apart, and the connection between them involves both the trunk lines and more than one switching node.

Routing system efficiency is determined by the traffic load that can be handled during the busiest times. Routing resiliency is critical to maintain a satisfactory level of service when either a traffic surge or equipment failure is experienced by the network.

Three approaches to signal routing are common. First, direct routing uses a fixed preestablished route that is setup for any pair of subscribers to follow. Second, with what is called alternate hierarchical routing, the switching nodes are arranged in a hierarchy that includes additional trunks beyond those required for a simple tree structure. The additional trunks provide alternate routes that may be used to compensate for entrance loads or normal route unavailability. Third, dynamic nonhierarchical routing is used in peer network architecture, that is between networks of about the same size and using similar protocols. The route between subscribers is dynamically chosen at call setup time based on traffic load and availability. [Ref. 11:p. 42]

(2) Signal Control. Circuit switching networks use what are referred to as control signals for call and network management, including call establishment, maintenance, and termination. Especially in a large circuit switching network, both call management and overall network management require that information be exchanged between users and switching nodes, among switching nodes, and between switching nodes and the network management center. Signal control is necessary for these processes to occur.

Control signals allow users to use voice communication to transmit information. They connect switching offices together and transfer information between switching nodes. These signals indicate when a call cannot be completed, generate a signal to make a telephone ring, transmit information used for billing purposes, and transfer status information concerning network trunks and other equipment for routing or maintenance purposes.

Four basic types of control signals are used in a circuit switching network. These are supervisory, address, call information, and network management control signals.

Supervisory control signals provide the mechanism for obtaining the resources to establish a call. These signals control the use of network resources. They also are used to collect and disseminate information concerning the status of a call or attempted call.

Address control signals provide the mechanism for identifying the subscribers or other users participating in a call or call attempt. Address signals originate with the caller. If more than one switching node is involved in the call setup, address control signals provide communication between switching nodes.

Call information control signals provide information to callers and operators relative to the establishment of a connection through a circuit switching network. The information is provided to both the call initiator and the recipient, and indicates the status of the call to the caller.

Network management control signals include those signals related to the ongoing operation and management of the network. They control the overall route selection process and modify the operating characteristics of the network in response to overload and failure conditions.

Network management status signals provide status information to network management centers and to other switching nodes. [Ref. 11:p. 54]

b. Message Switching Technologies

Circuit switching technology is constrained since both stations must be available at the same time for the data exchange. Resources must be available and dedicated throughout the network between the two stations. Message switching technology overcomes these constraints, making it useful for digital data exchange.

With message switching, it is not necessary to establish a dedicated path between two stations; the message is simply passed through the network from node to node. At each node, the entire message is received, stored, and then transmitted to the next node. This system is also known as a store-and-forward message system.

With message switching technology, the transmission unit is a well defined block of data called a message. In addition to the text to be transmitted, a message includes a header and a checksum. The header contains information regarding the source and destination addresses. The checksum is used for error control purposes. [Ref. 13:p. 26-3]

Message switching technology has a number of advantages.

- Line efficiency is improved.
- Both stations do not have to be available at the same time.
- The same message can be sent to many destinations.
- Message priorities can be established.
- When traffic is heavy, messages are still accepted; delivery may be delayed, but traffic continues to flow.
- Error control and recovery procedures are included.

- Messages sent to inoperative terminals may be intercepted and either stored or rerouted to other terminals. [Ref. 4:p. 199]

The disadvantage of message switching is that this technology is not suited for real time or interactive traffic. Delay time through the network is relatively long; delivery times have a relatively high variance. Thus this technology is not suitable for voice communications.

c. *Packet-Switching Technologies*

The technology of packet switching was developed to provide an efficient data transmission facility for WAN communication. With a packet-switched network, a source terminal, host computer, or data transmission station passes data over a network in the form of a "message." The message, along with its destination address, is sent to a local packet-switching node (PSN) computer. The PSN breaks the message into constant-sized "packets" of data. Each of these packets has the same destination address as the original message, plus a sequence number that indicates which piece of the whole message this packet represents. The packets are passed from PSN to PSN until they reach the destination PSN. [Ref. 12:p. 15.5.2]

A packet-switched network differs from a circuit-switched network (such as a telephone network) in that no predetermined, dedicated path exists for delivery of packet-switched data. The PSNs are capable of reliably and efficiently steering data packets through the network, avoiding traffic congestion and out-of-service nodes. Each packet takes the best route that it can find at the time, and all the packets in a given message do not necessarily take the same route. Once the packets arrive at the destination PSN, they are reassembled into the right sequence and are then delivered as a complete message to the destination host. [Ref. 13:p. 26-3]

Network PSNs are connected together via interswitch trunk lines, as shown as Figure 2-10. Packet switching provides a number of advantages. These include data rate independence, accommodation of bursty traffic, and flexibility. The U.S. DDN utilizes packet switching technology for data transmission.

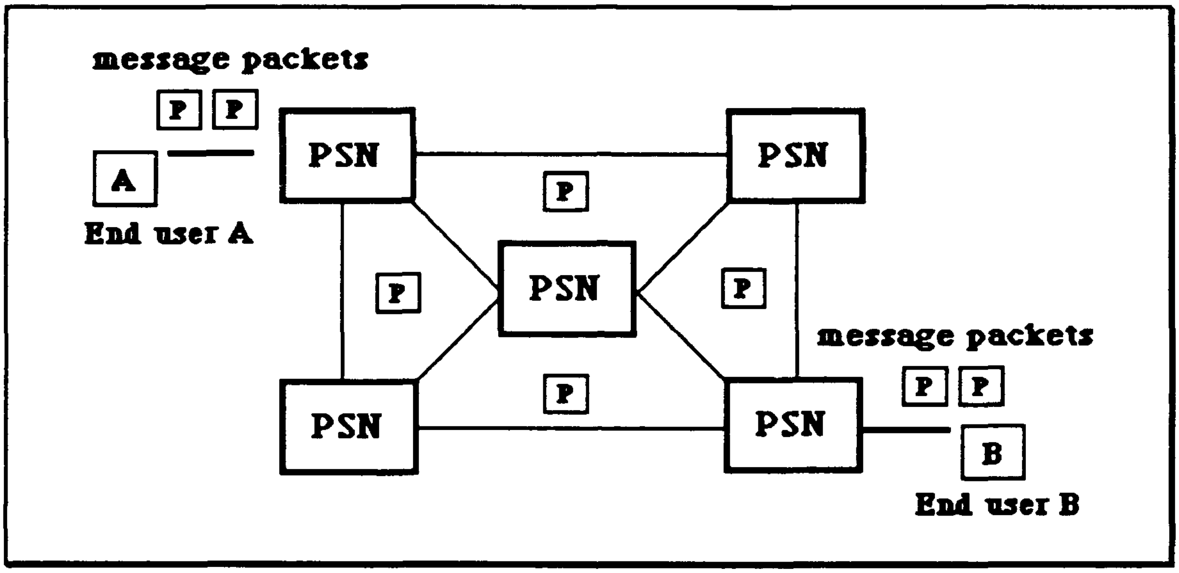

Figure 2-10. Generic Packet-Switching Network

(1) Packet Routing. Since the source and destination hosts or stations are not directly connected, the network must route each packet from node to node through the network. The dynamic routing capability of the system responds to outages of nodes or trunks by routing traffic around the outage on the next least-delay path.

The U.S. DDN uses what are called dynamic adaptive routing procedures. At each PSN, each incoming packet is time stamped with an arrival time. A route toward the packet's destination is selected, and a departure time is recorded when the packet is transmitted. [Ref. 14:p. 150]

If a positive acknowledgement that transmission may begin is returned from the next PSN, the delay for that packet is recorded as the departure time minus the arrival time plus transmission time and propagation delay. The node must therefore know link data rate and propagation time. If a negative acknowledgment comes back (the next PSN cannot accept the packet), the departure time is updated and the node tries again until a measure of successful transmission delay is obtained.

This procedure is both responsive and stable for reliable message delivery. Such routing can continue in the face of disruptions to individual nodes and links as long as some source-to-destination path is maintained. Network performance need not suffer significantly despite a reduced resource base, yet the addition of more switch nodes will enhance the capability of network service. [Ref. 4:p. 259]

(2) Traffic control. The amount of traffic entering and transiting a network must be regulated for efficient, stable, and fair performance. Traffic control is necessary on a packet-switching network to assure that a transmitting host or station does not overwhelm a receiving station with data. With some control procedures, the transmission medium between stations is referred to as a data link. Data link control usually manages the data flow between stations on one physical communication link.

The virtual-circuit service of the U.S. DDN provides two levels of traffic control for messages. One is referred to as an "entry-to-entry" technique. The DDN enforces a limit of eight messages in transit between any pair of stations or host computers. This prevents any host from flooding the network and overutilizing the resources. In order to resolve any resulting "deadlocks," a source node must reserve space for each message in advance, with a "require buffer space" packet. When a destination node receives this request and has available eight buffers for the eight packets that the message might contain, it returns an "allocation" packet.

After the entire message is received and reassembled, the receiving node sends back an acknowledgment known as a "ready for next" message. If the receiving node has buffer space for an additional message, it piggybacks an "allocation" packet with the "ready for next" message. Thus, during stream transmission, the source node need not send request packets. A time may come when the source has no messages to send but has collected one or more "allocation" permits. The source node is then obligated to send a "give back" packet to free up buffer space at the destination. [Ref. 4:p. 275]

The other DDN traffic control level is referred to as "datagram" service. For datagram service, no positive flow control is enforced. Rather, a destination node will discard packets (datagrams) for which it has no free buffer space. It is up to the source station to determine from the destination station if the datagram did not get through and to resend it if necessary. [Ref. 4:p. 279]

(3) Error control. Inevitably packets will be lost in a network. Some networks ignore this contingency; most take at least partial measures to alleviate this problem. Error detection procedures or automatic repeat requests are used to detect the bit errors and recover them.

The U.S. DDN exercises no error control for datagram service. Since the DDN uses datagrams internally, virtual circuits are maintained as long as there is some route from source to destination.

Error control is provided at the entry-to-entry message level. When a source node transmits a message (in up to eight packets) it retains a copy of that message, including its sequence number. If acknowledgment of receipt is not received within a certain time, the source node inquires of the destination node whether the full message was received.

It might be that the message got through, but the acknowledgment did not. If the source node gets a negative reply, it retransmits the message. If the source node fails to get a response from the destination node within a reasonable time, it returns an "incomplete transmission" message to the sending host. It is then up to the host to decide a course of action. [Ref. 4:p. 283]

d. Fast-Packet-Switching Technologies

Fast-packet-switching (FPS) technology adapts the technologies of packet switching to the high-speed digital signal transmission environment. It retains the advantages of both circuit switching and packet switching technologies while overcoming some of their weaknesses.

The key characteristics of the FPS approach include no node-to-node error control, no node-to-node flow control, end-to-end error control if necessary, and use of internal virtual circuits. An FPS facility requires that little or no time be spent on routing decisions once an external virtual circuit is set up; an internal virtual circuit is used instead. [Ref. 11:p. 102]

FPS technology can be used in place of circuit switching technology when voice signals can be digitized and transmitted as a stream of small packets. FPS technology requires rapid digitization. As a result, its delivery rates are constant. High-speed trunk lines are used to provide rapid transmission. Thus FPS can provide more efficient communications than circuit switching for bursty data traffic. [Ref. 11:p. 103]

The basic FPS packet format is shown in Figure 2-11. Flags are used to delimit each packet. A virtual circuit number is used for packet routing. A simple frame check sequence is used for error detection. Whenever an error is detected, the packet and its data are simply discarded. Flow control and error control thus are dispensed with. [Ref. 11:p. 104]

Flag	Virtual-circuit number	Data	Frame check sequence	Flag

Figure 2-11. Fast-Packet-Switching Packet Format

2. Network Transmission Media Technologies

The transmission medium forms the physical path between two users in a communication system. The quality of the communication depends both on signal quality and the transmission medium used. Transmission media can be categorized as unguided and guided.

a. *Unguided Signal Transmission Media*

Two basic types of unguided transmission media are in use: microwave and radio. From a practical standpoint, the principle difference between microwave and radio transmission is directionality. That is, microwave signals are focused and radio signals are omnidirectional.

Unguided communication frequency bands extend from 30 kHz (low frequency) to 300 GHz (extremely high frequency). For unguided media, the higher the center frequency of a signal, the greater the potential bandwidth and hence the greater the data rate. In general, at low frequencies (e.g., radio frequencies) signals are omnidirectional and at higher frequencies (e.g., microwave frequencies) signals can be focused in a desired direction, usually toward a repeater station or specific receiving station. [Ref. 13:p. 1-3]

(1) Microwave Signals. The microwave frequency spectrum ranges from approximately 2 GHz to 40 GHz. Microwave signals are used primarily for point-to-point (line-of-sight) transmission due to the ability to generate highly directional beams. These higher frequency signals result in greater potential signal bandwidth which permits greater data transmission rates. [Ref. 4:p. 57]

(2) Radio Signals. Radio signals are radiant waves of low frequency energy transmitted into space. Radio signals are sent from transmitting antennas as either sky waves or ground waves. "Radio" is a general term sometimes used to encompass the entire electromagnetic frequency spectrum with wavelengths longer than 1 cm. It also can be defined in a more restricted sense to cover the very high frequency (VHF) and part of the ultra high frequency (UHF) bands. Frequencies ranging from 30 MHz to 1 GHz are effective for broad area communications. [Ref. 4:p. 61]

b. Guided Signal Transmission Media

There are three principle types of transmission media used for guided signals: twisted pair wires, coaxial cable, and optical fiber cable. For computer and network communications, each has different characteristics related to their transmission functions, as shown in Table 2-1. [Ref. 4:p. 47]

(1) Twisted Pair Wires. Twisted pair transmission media consist of two insulated copper wires that act as a single communication link.

This technology can be used for both analog and digital data transmission. It provides the communication medium for most telephone systems and most intrabuilding system, and delivers data rates of approximately 4 Mbps. [Ref. 4:p. 47]

TABLE 2-1 TRANSMISSION CHARACTERISTICS OF GUIDED MEDIA

Transmission Medium	Total Data Rate	Bandwidth	Repeater Spacing
Twisted pair	4 Mbps	250 kHz	2-10 km
Coaxial cable	500 Mbps	350 MHz	1-10 km
Optical fiber	2 Gbps	2 GHz	10-100 km

(2) **Coaxial Cable.** This guided signal medium consists of two conductors inside a shielding cable. Its construction permits it to carry signals over a wider range of frequencies. Coaxial cables are used for long-distance telephone and television transmission, local area networks, and short-run system links. Currently coaxial cable is the only transmission medium that can provide the bandwidth requirements for LAN backbones. [Ref. 15:p. 418]

(3) **Optical Fiber.** An optical fiber is a thin, flexible glass or plastic strand capable of conducting an optical ray. An optical fiber cable is cylindrical in shape and consists of three sections. The core is the inner section and consists of one or more very thin fibers. The cladding surrounds the core. It consists of a glass or plastic coating that has optical properties different from those of the core. The jacket is the outer layer that surrounds a bundle of cladded fibers. Made of plastic or similar materials, it protects the fibers and cladding against environmental hazards. [Ref. 4:p. 53]

Optical fiber cables are considered to be either multimode or single mode. With multimode fibers, light paths zig-zag through the fiber according to the angle of the ray's propagation and the reflective properties of the fiber. With single mode fibers, the rays follow a single direct path through the fiber core. The result is increased distances between repeaters and increased bandwidth. Thus multimode cable is used primarily for short and medium distance applications, with single mode used for long-haul applications. [Ref. 16:p. 33]

In an effort to standardize optical fiber technology, the Fiber Distributed Data Interface (FDDI) standard has been adopted by the American National Standards Institute. The standard specifies that optical fiber media will include physical and data link layers capable of operating at 100 Mbps when used in a ring topology.

Fibers meeting the FDDI standard will likely become the preferred transmission media for LANs of the future. Such systems can provide both the high bandwidth and low latency needed to match the increased capacity of future personal computers. Fiber optic backbones generally can provide a better transmission environment, including high date rates, low bit error rates, and low signal attenuation. [Ref. 15:p. 569]

c. *Advantages and Disadvantages of Various Media*

(1) Advantages and Disadvantages of Unguided Media. Unguided media, both microwave and radio, suffer from a limited data rate due to their fundamental characteristics; that is, bandwidth is limited by where they operate in the frequency spectrum. Attenuation from internal and external noise also limits data rates. However, unguided media still remain popular for various applications. These include point-to-point terrestrial digital radio, digital mobile radio, digital satellite communications, and deep-space digital communications. [Ref. 7:p. 120]

Unguided transmission media are especially good for transmitting and receiving data over long distances. This includes communication between two terrestrial end-users, particularly on sparse routes where the total communication traffic is small.

One of the most appealing uses for unguided transmission media is for communication with people or vehicles on the move. Guided transmission media cannot be used to provide point-to-point links for two mobile end users. Unguided transmission media are the only practical ways to provide this type of communication. [Ref. 7:p. 126]

(2) Advantages and Disadvantages of Guided Media. Currently, the backbones of most networks use twisted pair wires or coaxial cable for signal transmission. These do not always provide the flexibility or expandability needed for future applications and user demands. Generally, troubleshooting, system management, and maintenance are difficult and costly. [Ref. 4:p. 50]

Among guided media, twisted pair wire transmissions are limited in distance, bandwidth, and data rate. Higher performance requirements can be met by coaxial cables, which provide higher throughput to support a large number of devices and to span greater distances. Coaxial cable is used to transmit both analog and digital signals. Its frequency characteristics are superior to those of twisted pair wires Thus cable can be used effectively at higher frequencies and data rates. The principle constraints on coaxial cable performance are attenuation, thermal noise, and intermodulation noise. [Ref. 4:p. 51]

Fiber optic guided media have several advantages over coaxial cable.

- Fiber optic media can be installed in much smaller spaces than coaxial cable. The fiber systems are approximately one-seventh the weight and one-twentieth the size of coaxial cable.
- Costs for fiber optic and coaxial cable on a per foot basis are approximately the same. However, since the bandwidth of fiber optic materials is so much greater than coaxial cable, the cost per megabyte of fiber optic systems is less than for coaxial cable. As technology has improved, the cost of purchasing and installing fiber optic systems has decreased, while the cost of coaxial cable has remained approximately the constant.
- Fiber optic systems have a much greater bandwidth than coaxial cable. Fiber optic systems in use today have bandwidths of up to 580 MHz. Systems under development will reach bandwidths of 2 GHz. Coaxial cable has a maximum bandwidth of 500 MHz, with commercially available systems limited to around 100 MHz.
- Fiber optic systems have a very low bit error rate compared to coaxial cable.
- Fiber optic systems have very low attenuation or signal loss. Compared to coaxial cable, a fiber optic system requires up to six times fewer repeaters than does a comparable coaxial-based system.
- Fiber optic systems are immune to both electromagnetic interference and radio frequency interference, unlike coaxial cable. Because fiber optic systems use light instead of electrical pulses to transmit the signal, electromagnetic and radio signals have no effect on transmission quality or other characteristics.
- Fiber optic systems emit no electrical radiation and are almost untappable without detection. The location of breaks in a fiber optic cable can be detected to within a few inches. [Ref. 16:p. 33]

The disadvantages of fiber optic systems are few. They are most often criticized for complexity in connecting and splicing. However, this problem essentially has been solved by modern techniques and standards for connectors and tapping methods. [Ref. 16:p. 34]

III. UNITED STATES DEFENSE DATA NETWORK

A. OVERVIEW OF THE U.S. DEFENSE DATA NETWORK

The U.S. DDN has been designed to meet DoD requirements for a secure command and control communication network. This common-user worldwide data communications network allows communications that range from the most mundane matters of logistics to critical intelligence data transmitted among mainframe systems at various security levels.

The DDN is a kind of data communication network known as a packet-switching wide-area network. Users connect to the network to send and receive messages via a network access component. The DDN is designed to provide a low risk, cost-effective system that not only satisfies current requirements but is easily expandable and adaptable to satisfy requirements projected for the future. The DoD has committed to the DDN because it offers significant cost savings, interoperability, survivability, and reliability [Ref. 12:p. 15.5.1].

The DDN has successfully proven that computers made by various manufacturers, of various sizes, and with different operating systems can communicate with each other across a network. DDN users can share programs and can communicate through the network with each other at a long distances. This offers two significant advantages to its subscribers and to the government.

- The cost of data communications is reduced by sharing communication lines, communication equipment, and network control facilities.

- Otherwise incompatible subscriber terminals and hosts can communicate over the network, supporting the DoD goal for "interoperability." [Ref. 12:p. 15.5.1]

B. DDN HISTORY AND DEVELOPMENT

The development of the DDN began in the early 1960s with the first Automated Digital Network (AUTODIN I) message-switching system. The first packet-switching network was designed under a 1969 Defense Advanced Research Projects Agency research and development program. This latter network was designated the ARPANET, and its packet-switching technology has proven to be highly reliable [Ref. 31:p. 121].

ARPANET originally was a network used for research and development. As time went on, users with operational requirements also began to use the network. Because operational users, including various government departments and contractors, continued to increase, the Defense Communications Agency (DCA) took responsibility for the network's operation in 1975.

By the 1980s, the requirements for the military communication network were changing very fast. This rapid change, plus increasing costs, affected the original DoD plans related to AUTODIN. AUTODIN's small number of nodes did not satisfy current survivability requirements. Increased common carrier costs made long access lines to the small number of nodes particularly expensive. In addition, the ability of the switches to carry sensitive traffic securely appeared doubtful. [Ref. 31:p. 121]

In September 1981, the Director of the DCA initiated a study to define a survivable common-user data communications system. Two teams were tasked to develop the system. One of these teams developed a network plan based on AUTODIN message-switching technology. The second team developed a plan using ARPANET packet-switching technology.

In April 1982, the Department of Defense decided to terminate research related to development of AUTODIN II, and determined that the national DDN would be based on ARPANET technology. Guidance from the Secretary of Defense was provided as follows.

> All DoD ADP systems and data networks requiring data communications services will be provided long-haul and area communications, interconnectivity, and the capability for interoperability by the DDN. Existing systems, systems being expanded and upgraded, and new ADP systems or data networks will become DDN subscribers. All such systems must be registered in the DDN User Requirements Data Base. [Ref 17:p. 1]

Currently the DDN consists of several networks, as shown as Figure 3-1 [Ref. 18:p. 15.1]. Each network has its own mission and operates independently from the others. Each network also operates at its own security level. The MILNET, a military operational communications network, and the ARPANET, a military research and development network, constitute the unclassified segment of the Defense Data Network. The classified segment of the DDN consists of several independent networks. These include the Defense Integrated Secure Network (DISNET), the Strategic Air Command Digital Information Network (SACDIN), the Secure Compartmented Information Network (SCINET), and the Intercomputer Network Communication Subsystem (WIN).

The DDN's backbone structure and connections are shown in Figure 3-2 [Ref. 18:p. 15.1.4]. Users may do unclassified work from individual terminals on computer "host" systems that are attached to major Terminal Access Controllers (TACs) or to smaller Mini-TACs. The TACs allow access to the DDN system and are controlled from the DDN Monitor Center. Internet

Private Line Interface (IPLI) devices perform data encryption, as needed. The DDN also is connected to other networks via special computers known as gateways.

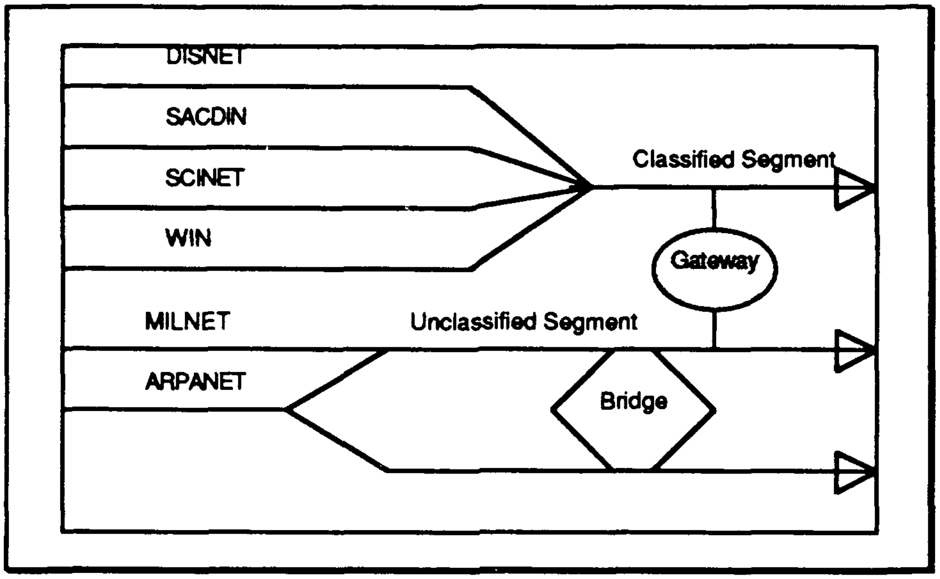

Figure 3-1. The Primary Components of the U.S. DDN

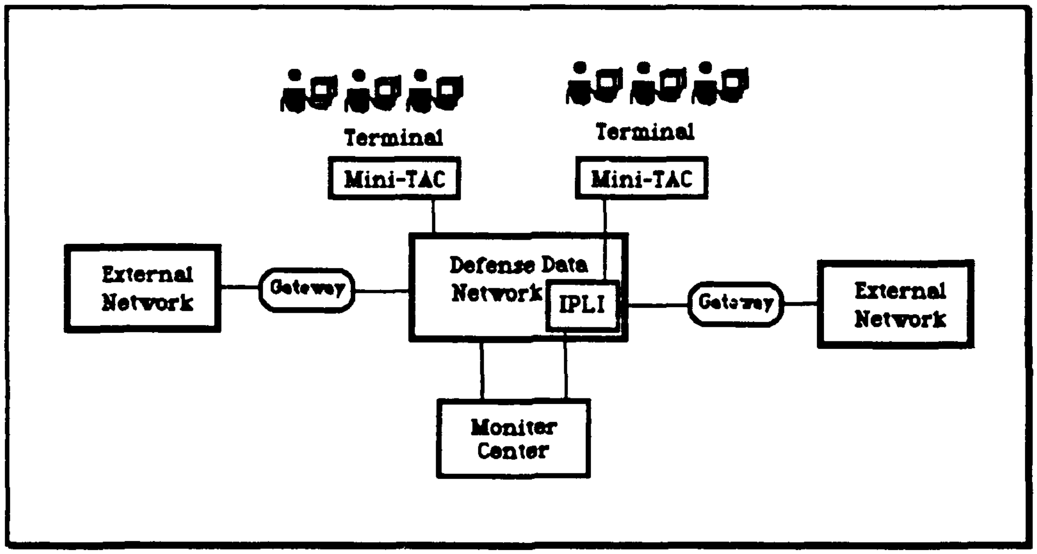

Figure 3-2. DDN Backbone Equipment and Connections

C. DDN SERVICES AND BENEFITS

1. Services

The DDN is currently a very large military common-user data communications internetwork, designed for continuous operation (24 hours a day, seven days a week) throughout the world. It might be thought of as an "umbrella" network composed of several large segments or subnetworks. It is designed to support military operations and intelligence systems as well as general purpose automated data processing (ADP) systems and data networks having long-haul data communications requirements.

Currently DDN users include various military departments, DoD agencies, intelligence organizations, and DoD contractors. The Marine Corps uses the network for logistics and administrative operations. The Air Force is upgrading its personnel system for compatibility with the DDN. The Army Inspector General's Management Information System is being connected to the network, and the Navy's Regional Data Automation Center also has registered with the network. Many organizations already use the DDN for electronic mail. Within the next few years, most armed forces management functions, including payroll, logistics, medical records, personnel, intelligence, and C3I, will be maintained on the network [Ref. 31:p. 122].

2. Benefits

a. Cost Savings

The DDN reduces the cost of data communications by sharing communication lines, communication equipment, and network control facilities. It offers a cheaper and faster data communication method for a long distances, especially when military communications are heavy. Since many of the DoD's largest ADP systems have joined the hundreds of other computers already using the network, the DDN has become a global operational resource. It permits otherwise incompatible subscriber terminals and hosts to communicate over the network, to help achieve the DoD goal of "interoperability." [Ref. 19:p. 22]

b. *Survivability*

The DDN is designed for survivability. Since it consists of a large number of fixed switching nodes along with a few transportable ones, there are multiple paths through the trunking system to all possible points in the network. Thus the DDN can be utilized for the missions and against the threats defined by the U.S. Joint Chiefs of Staff. Each mission is described in terms of a "stress level." Survivability measures are built in at the network or system level, node level, and user level to insure that the DDN can meet military requirements in response to each level of stress. Five such levels of stress have been defined, as shown as Table 3-1 and described below. [Ref. 20:p. 11]

(1) Peacetime Readiness. Threats related to peacetime operations are equipment failure, power failure, natural disasters, civil disorder, and outage of trunks and access lines. The mission of the DDN is to provide continuous, reliable user service while supporting command, control, and intelligence traffic and DoD administrative users. The precedence and preemption capabilities of the network insure that the critical traffic is handled first. If the system's trunk lines are lost they will be replaced automatically with dial-up-and-hold circuits.

TABLE 3-1 DDN ROLE UNDER VARIOUS MISSION STRESS LEVELS

Stress Level	Primary DDN Roles
Peacetime	Support command, control, and intelligence traffic and DoD administrative users.
Crisis and Preattack, and Theater Non-Nuclear War	Support the above, plus surge requirements, handled according to established procedures.
Early Trans-Attack	Support critical C3I traffic
Massive Nuclear Attack	Support critical traffic as able.
Postattack	Possess capability to initiate reconstitution from the surviving fragments of the network. Support the Defense Communications system (DCS) as part of Network Communications System (NCS) reconstituting national communication

(2) **Crisis and Preattack, and Theater Non-nuclear War.** The scenario of crisis and preattack has been defined by the DoD to include international crises related to conventional warfare within a threat situation, prior to an attack. Such situations are expected to cause network traffic to increase sharply. The threats to the network are equipment failure, surge in traffic loads, sabotage, and conventional weapons targeted against the network and its users in the theater. The DDN mission is to maintain the network, continuing to provide full services to the planned subscribers in spite of increased load and decreased capacity. Precedence and preemption capabilities insure that critical users have priority for service.

(3) **Early Trans-attack.** During this period, the major threat to the network is limited use of nuclear weapons against the system. Critical nodes damaged or destroyed would be replaced by reconstituted nodes. The mission of the DDN is to support its critical command, control, communication, and intelligence information functions without any degradation by using precedence and preemption procedures.

(4) **Massive Nuclear Attack.** The threat at this level is escalated by the extensive use of nuclear weapons against the network. The mission of DDN at this stress level is to maintain network traffic as long as it can and restore network services promptly. It is expected that many network nodes may malfunction after a massive nuclear attack.

(5) **Postattack.** Following the continued use of nuclear weapons against the surviving system, the network must possess the capability to reconstitute itself from surviving fragments and must provide support to the reconstitution of the DoD and national communications. [Ref. 14:p. 149]

c. *Security*

Several safeguards are used to protect the security and privacy of DDN subscriber traffic. Packet switches and TACs are located in facilities that are physically secure. Various security levels are provided through rigorous separation of classified user communities working at different classification levels.

The DDN also has been provided end-to-end encryption by Internet Private Line Interface (IPLI) devices. The IPLI system is situated between the host or mini-TAC and its switching node. Messages are encrypted via the IPLI as they pass through the switch and decrypted as they are passed to their destinations shown as Figure 3-2. [Ref. 20:p. 99]

d. *Reliability*

Error detection techniques provide the DDN's high level of reliability. The chance of an error being transmitted through the DDN without being detected is extremely small. All detected errors automatically result in the retransmission of the packet in error; this process is invisible to the user. [Ref. 13:p. 7]

e. Interoperability

By requiring that all computer hosts use suitable software and protocols, the DDN provides excellent computer compatibility and interoperability for the DoD community. The DDN supports many types of computers, operating systems, and terminals that can communicate via compatible host systems. [Ref. 17:p. 13]

Interoperability also means that electronic mail messages can be sent between users on widely differing computers. File Transfer Protocol (FTP) permits the transfer of data files between various computers located many miles apart. In addition, Telnet protocols allow a user on one DDN terminal to log on to another, far-distant host computer to which he has access in order to make use of programs and files located there.

IV. INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

A. ISDN OVERVIEW

For more than a century, the primary communication system between two end users has been the traditional telephone system. This system was designed for analog voice signal transmission only, not for modern data transmission, teletex, facsimile, videotex, and teleconferencing technologies.

Communication networks now are expected to handle a variety of data traffic types. These cover a range of applications as diverse as very low bit-rate control and alarm channels for the home and business, interactive information services, electronic mail, digital voice, facsimile, file transfer, and wideband digital video services. [Ref. 3:p. 661]

Computer and communication technology has improved rapidly. Users now demand far more services than can be provided via a traditional single-purpose network. Original telephone systems have been replaced with advanced digital systems. Digital data, digital voice, and digital images now all can be transmitted by telephone. Systems with these capabilities are referred to as integrated services digital networks (ISDN). Some of these advanced services are already available in primitive form, but these exist on different networks and are poorly integrated.

To overcome these problems, the International Telegraph and Telephone Consultative Committee (CCITT) is overseeing the standards and protocols for interconnected ISDNs. Eventually a worldwide ISDN public telecommunications network is foreseen, providing services to meet a wide variety of user needs. The ultimate function of ISDNs is to satisfy the increasing demand services for efficient and timely collection, processing, and dissemination of information. [Ref. 11:p. 3]

ISDNs are characterized by standardization of user interfaces and are implemented as a set of digital switches and paths supporting a broad range of traffic types and providing value-added processing services. These traffic types and services include teleconferencing, private branch exchange (PBX), teletex, facsimile, and videotex. ISDNs may be implemented in a variety of configurations according to specific national policy, the state of technology, user needs, and the existing equipment of the customer base. Figure 4-1 illustrates these concepts.

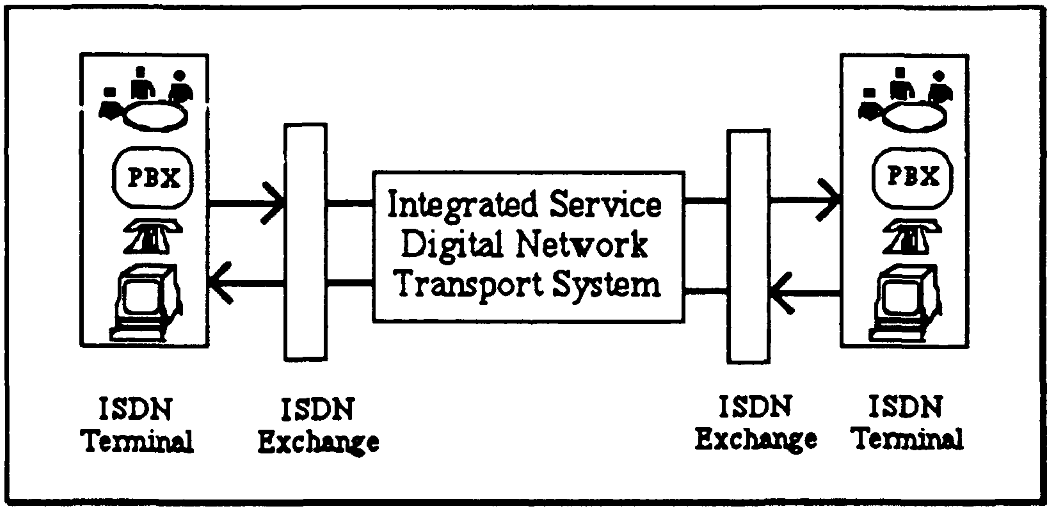

Figure 4-1. ISDN Transport, Exchange, and User Equipment

ISDN characteristics, as defined by the CCITT, are well established. The main feature of the system is support of both voice communication and nonvoice communication applications using a limited set of interfaces and standardized data transmission facilities. The ISDNs will support a variety of applications including both switched (circuit switching and packet switching) and non-switched technology in order to achieved the necessary connections between users. Any component system of the ISDN is expected to use intelligent switching nodes in the network to provide sophisticated services, network maintenance, and management capabilities.

B. ISDN HISTORY AND DEVELOPMENT

The evolution of ISDN concepts has been defined by the CCITT. The system is based on concepts developed for telephone ISDNs. It may evolve by progressively incorporating additional functions and network features. These include features of other dedicated networks such as circuit switching and packet switching for data, in order to provide for new and improved services.

The transition from an existing network to a comprehensive ISDN may require a period of time extending over one or more decades. During this period, arrangements must be developed for the interworking of services on ISDNs and services on other networks.

In the evolution towards an ISDN, digital end-to-end connectivity will be obtained via plant and equipment used in existing networks, such as those used for digital transmission, time-division multiplex switching, and/or space-division multiplex switching. In the early stage of the evolution of ISDNs, some interim user-network arrangements may need to be adopted in certain countries to facilitate early penetration of digital service capabilities. An evolving ISDN may also include at later stages switched connections at bit rates higher and lower than 64 kbps. [Ref. 4:p. 595]

C. ISDN TECHNOLOGY

Although the ISDN is based on telephone networks, its development and structure have been strongly affected by non-voice services. ISDN is supported by integrated digital network (IDN) technology, from which it has evolved [Ref. 11:p. 111]. The technology underlying ISDN has been driven by market pressures to reduce the cost of both voice and non-voice telecommunication. ISDN technology is based on digital transmission and switching technologies. These have been tailored as necessary to build an all-digital telecommunications network.

ISDNs are designed to support a completely new physical connection for the user, a digital subscriber loop that links the end user to a central or end office, as shown as Figure 4-1. ISDNs will provide circuit-switched and packet-switched transmissions at 64 kbps, their basic rate of data transmission.

ISDNs provide end-to-end digital 64 kbps bit-rate connections between users; no analog signals are used in the link. ISDN brings digital transmission all the way to the user premises using digital subscriber loops that link an ISDN end user terminal to the ISDN exchange. Services dependent on a digital interface, such as data, can be provided directly without an analog-to-digital modem. Also 64 kbps bit rates can provide more services than the analog-to-digital modem for data transmission. ISDN offers an opportunity for integration of many services short of full-motion video. [Ref. 11:p. 168]

Some ISDN communication services require circuit-switching technology, some packet-switching technology, and some hybrid-switching technology. Packet switching must be performed at much higher bit rates for use with integrated services such as video than it originally was designed for. [Ref. 11:p. 66]

A layered protocol architecture is being developed for user access to ISDN services. This architecture can be added to the OSI model to provide a number of advantages. The existing OSI standards may be used on ISDN. New standards can be based on existing standards or can be developed and implemented independently for various layers and for various functions within a layer.

The digital transmission line between ISDN users will be used to carry a number of communication channels. Several channel types have been standardized.

- 64 kbps digital pulse-code modulation (PCM) channel for voice or data
- 16 or 64 kbps digital channel for out-of-band signaling
- 384, 1536, or 1920 kbps digital channel
- 4 kHz analog telephone channel
- 8 or 16 kbps digital channel
- 64 kbps digital channel for internal ISDN signaling [Ref. 4:p. 597]

The transmission structures of all access links are designed to utilize the three primary types of channels. These three channels are grouped into transmission structures that are offered as a package to the user. [Ref. 8:p. 103]

1. B Channel: 64 kbps

The ISDN B channel has been assigned as the basic user channel. It can be used to carry digital data, digital voice, PCM-encoded digital voice, or a mixture of low-rate traffic that includes digital data and digital voice encoded at a fraction of 64 kbps. Three kinds of connections can be made via the B channel. The first connection is circuit-switched, using the same technology as the traditional telephone system. Second, the packet-switched connections allow the users to connect to a packet-switching node for information exchange. Third, semipermanent connections allow users to communicate using a prior set up arrangement. [Ref. 4:p. 600]

2. D Channel: 16 or 64 kbps

The ISDN D channel has two functions. First, it carries signalling information to control circuit-switched calls on associated B channels. Second, the D channel may be used for packet-switching or low-speed telemetry at times when no signalling information is waiting. [Ref. 4:p. 600]

3. H Channel: 384, 1536, and 1920 kbps

This channel has been used to provide for information transmission at high bit rates. It is used for fast facsimile, video, high-speed data, high-quality audio, and multiple information streams. The higher bit rates result in correspondingly shorter delays in assembling packets, a factor that is of importance in voice and interactive services. [Ref. 4:p. 600]

D. ISDN SERVICES AND BENEFITS

1. Services

The ISDN will provide a variety of services by using data, voice, and image transmission technologies. Most of these services can be provided with a transmission capacity of 64 kbps or less. Since some services need higher transmission rates, these services will be provided via the Broadband ISDN (BISDN) standard. BISDN, like ISDN, is an industry standard, defined in CCITT Recommendation I.121 to support the emerging demand for high-bandwidth services. [Ref. 11:p.168]

Voice, digital data, text, and image transmissions can be provided by ISDNs. Most of these services can be provided with 64 kbps data transmission rate. The basic candidate services of ISDN are shown in Table 4-1. Several of the most important services are facsimile transmissions, and teletex, videotex, and teleconferencing services.

TABLE 4-1 CANDIDATE SERVICES FOR ISDN BANDWIDTH

	Bandwidth	
Service	**Digital voice (64 kbps)**	**Wideband (>64 kbps)**
Telephony	Telephone, leased circuits, information retrieval	Music
Data	Packet-switched data, circuit-switched data, leased circuits, telemetry, funds transfer, information retrieval, mailbox, electronic mail, alarms	High-speed computer communication
Text	Telex, teletex, leased circuits, videotex, information retrieval, mailbox, electronic mail.	
Image	Facsimile, information retrieval, surveillance	TV conferencing, teletex, videophone, cable TV distribution

a. Facsimile Transmission

Facsimile services are used for transmission and reproduction of graphic, handwritten, and printed material. This type of service has been available for several years, but it has suffered from the limitations of the analog telephone network. Digital facsimile standards are now available and can be used to transmit a page of data at 64 kbps in 5 seconds [Ref. 11:p. 168]. Using this service, an image is scanned and digitized electronically. The resulting bit stream is then transmitted to the destination and then redrawn on a piece of paper. Facsimiles need not be restricted to the copying of paper documents, but are generally useful for transmitting any image. This technique currently requires high bandwidth frequencies, but potential services under development will be able to use low bandwidths. [Ref. 11:p. 198]

b. Teletex

Teletex is essentially a form of electronic mail for home and business. Digitized messages .re sent from one location to another cheaply and rapidly. The technique has been designed for economical use with the telephone system. Terminals usually are suitable only for text and some basic graphics. These include contracts with handwritten signatures, charts, diagrams, blueprints, illustrations, and so on. [Ref. 11:p. 209]

c. Videotex

Videotex is an interactive information retrieval service. A page of data can be transmitted via an interactive process to a remote database by a person at a terminal that provides information retrieval services. For example, a customer can buy a product by typing its order number, and have it charged to a credit card or telephone bill. [Ref. 4:p. 591]

d. Teleconferences

Electronic meetings are considered to be among the most advanced communications technologies. Meetings can be held between two or more remote locations. Large groups of people thus can share remote resources. Basically, teleconferencing systems have been divided into four categories. Audio conferencing is the basic form, and uses voice transmissions only. Audio-graphic conferencing provides transmission of graphs, charts, diagrams, and text, as well as voice. Computer conferencing permits two computers to link to each other, for the exchange of data only; voice transmissions are not included. Video conferencing combines audio and visual communication for real-time information transmission. [Ref. 32:p. 18-4]

2. Benefits

ISDN systems benefit customers, network providers, manufacturers, and others. The principle benefits of ISDN to the customer are cost savings and flexibility. The user of ISDN does not have to buy multiple services to meet a variety of demands, because ISDN has integrated voice and nonvoice services on a single communication network. ISDNs allow the user to purchase what actually is needed according to the user's own requirements. Also competition among equipment venders will result in advantages that include low price and wide availability of services. [Ref. 4:p. 591]

Since venders compete with each other, the prices of equipment such as digital switches and digital transmission lines are lower in cost than before. ISDN standards support standardized equipment and a large potential market for services. Interface standards permit flexibility in selection of suppliers, consistent control signaling procedures, and technical innovation and evolution within the network. [Ref. 11:p. 158]

ISDN also provides the manufacturers an environment in which they can focus research and development on technical applications and be assured that a broad potential demand exists. End users benefit because they will not be required to buy special equipment or terminal devices in order to gain access to particular services.

Two of the principal benefits to the user of ISDN systems are cost savings and flexibility. The integration of voice and a variety of data on a single transport system means that the user does not have to buy multiple services to meet multiple needs. ISDN allow the user to access a menu of different services through a common set of switches and transmission facilities.

V. PROPOSED FRAMEWORK FOR AN R.O.C. IDCN

A. OBJECTIVE OF AN R.O.C. ARMED FORCES IDCN

As discussed in Chapter I, the current R.O.C. Armed Forces C3I system is a conglomeration of diverse subsystems. No comprehensive system has been developed to meet C3I requirements. Telecommunication systems consist of a large number of individual networks and links, each designed to optimize a specific task and operate independently within a given transmission medium.

Changing requirements and increasing costs have affected the ability of the R.O.C. Armed Forces to obtain adequate communication systems. The austere environment in which the R.O.C. Armed Forces must operate makes it especially difficult to develop a satisfactory C3I system. Yet the mission of the Armed Forces makes it imperative that a C3I network be available, one that is fast, secure, reliable, flexible, survivable, and inexpensive to operate.

It is proposed that the R.O.C. Armed Forces remedy their communication problems through development of a comprehensive, integrated defense communication network, an IDCN. The primary function of the IDCN is to provide long-haul data, voice, and image transportation through an integrated network to support C3I requirements. Using modern computer communication technology, the IDCN could provide a number of C3I-related services including electronic mail, voice communication, videotex, and teleconferencing.

An IDCN could provide resource sharing that results in rapid, secure, and convenient intradepartmental and interdepartmental data sharing. Electronic mail and voice mail would ensure that users communicate their ideas and information rapidly and easily. Through modern voice and data transmission technologies, the IDCN could provide greater levels of efficiency for its users. Resource sharing and time sharing could result in significant cost savings for the R.O.C. Armed Forces. A well-designed IDCN can satisfy wartime survivability requirements. Overall, an IDCN will meet C3I requirements for communication speed, security, reliability, flexibility, survivability, and cost savings.

Digital communication technology can improve the speed of communication between users significantly. Modern computing security technology can provide measures such as physical, line, and end-to-end encryption to improve communication security. Computer communication technology will improve reliability. Interoperability that results from communication standards will result in greater flexibility. System redundancy and network interoperability will increase survivability. Sharing of resources and facilities will significantly cut costs.

B. EXISTING COMMUNICATION RESOURCES

As discussed in Chapter II, the trend in both military and nonmilitary communications is away from analog and towards digital communication technology. Voice, data, and image information are being transformed to digital format and integrated for transmission over broadband networks.

R.O.C. commercial telecommunication systems have been improved significantly over the last few years, using modern technologies and equipment obtained from the U.S. and European countries. International telecommunication systems are accessible throughout the area. Data, voice, and image transmission, including public data information systems, videotex, E-mail, data communication service, and teleconferencing are available. The range of services is illustrated in Figure 5-1.

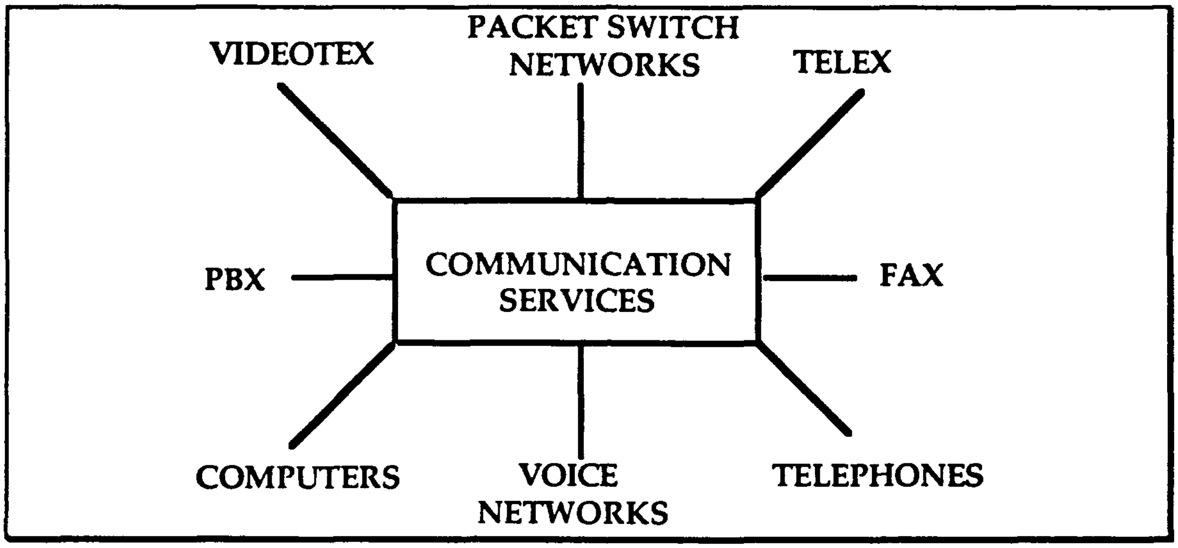

Figure 5-1. Existing R.O.C. Telecommunication Services

An existing commercial R.O.C. wide area (long-haul) network now covers the entire Republic, including the islands of Kin-Men, Ma-Tue, and Pong-Hu, as illustrated in Figure 5-2. The existing R.O.C. packet-switching data communication system is shown in Figure 5-3. Communication quality has been improved through an optical cable transmission system, under development throughout the entire area. ISDN technology has been introduced, and is expected to be in use in 1990.

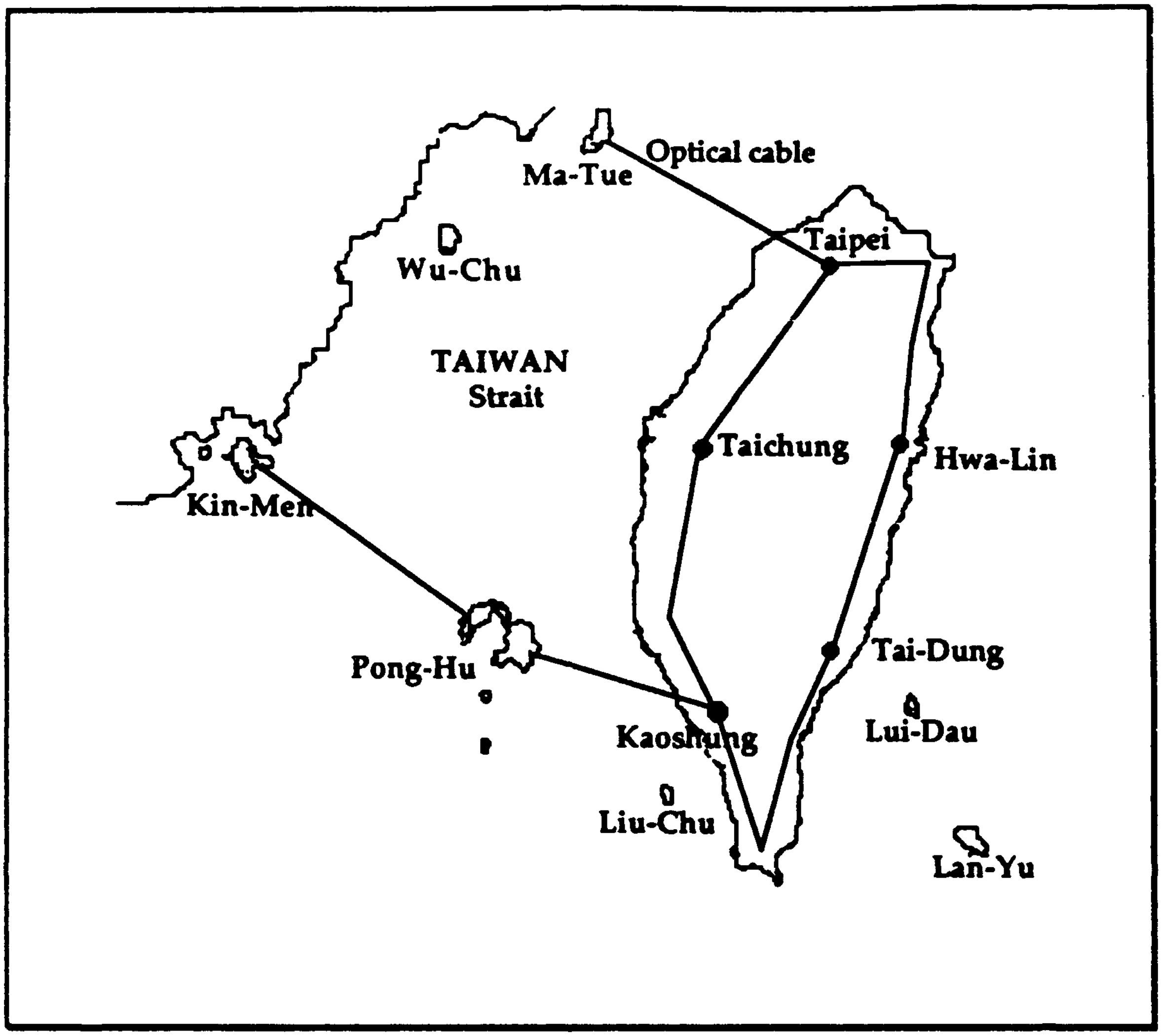

Figure 5-2. R.O.C. Wide Area Network

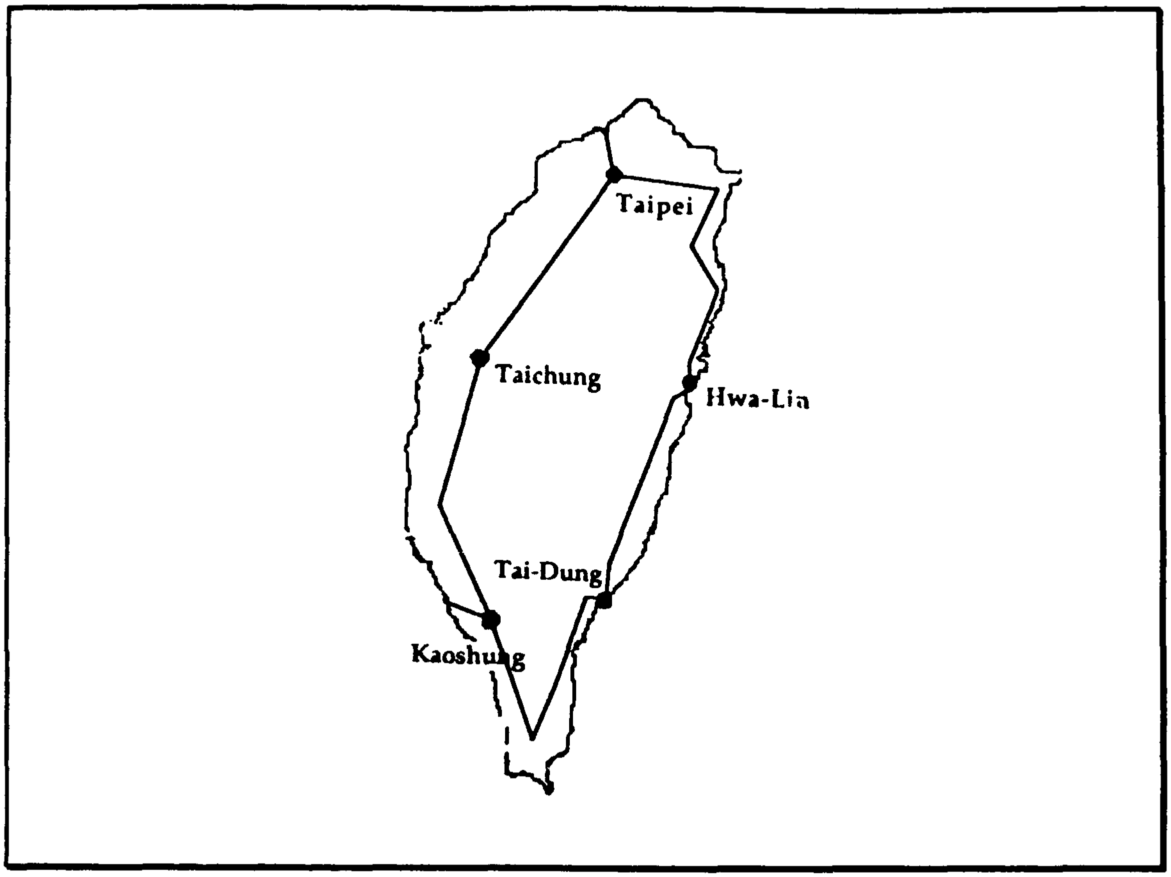

Figure 5-3. R.O.C. Packet-switching Data Communication System

C. PROPOSED IDCN TECHNOLOGIES

Using modern digital data communication technology, the IDCN can provide an integrated communication environment for the R.O.C. Armed Forces, as needed to achieve their defense mission. The fundamental technologies that are proposed as ingredients of the IDCN are digital data communication technologies, network technologies, network components technologies, and ISDN technologies. These technologies have been discussed in Chapter II and Chapter IV and are in wide use today.

1. Digital Data Communication Technologies

Digital data communication technologies include data encoding, data compression, data transmission, and multiplexing. Digital data encoding techniques can improve data accuracy, while eliminating redundant data entry and lost data. Errors related to data entry, transmission, and processing can be drastically reduced. Data compression and data transmission techniques will improve the speed of military communications. Multiplexing techniques will improve network efficiency.

2. Network Technologies

Network technologies include protocols, topologies, and types of networks. The well-established OSI model provides a common basis for the development of new systems through standards for devices and interconnections. OSI protocols provide for physical connections between end users and transmission of data across the physical transmission resources. The OSI model can be used as the basis for connecting various systems of the IDCN for distributed applications and processing.

The IDCN topological design should result in sufficient trunking and switching resources to handle all expected long-haul data flows. The best topology is directly related to the total volume of traffic. The four types of topologies discussed in Chapter II have various advantages and disadvantages as a function of transmission medium and traffic type. IDCN services probably will employ ring, bus, tree, and star topologies for various processes carried out in the network.

The overall IDCN WAN probably will include several LANs. Thus both LAN and WAN technologies must be considerd during system development.

3. Network Components Technologies

Network components technologies include switching technologies and transmission media technologies. In order to meet all requirements, circuit switching, message switching, packet switching, and fast packet switching technologies can be used for various functions in the IDCN.

Packet switching technology is advantageous when large numbers of users will share a common set of high bandwidth, high quality transmission facilities. This technology is expected to minimize the costs of military communication. Circuit switching technology also will be required, however, to provide efficient real-time services.

Transmission media provide the physical channels used to interconnect nodes in the network. For the IDCN, both guided transmissions and unguided transmissions will be needed. Unguided transmission media, including signals from satellites, are required for communications among mobile military units. Guided transmission media provide better communications among various land bases.

4. ISDN Technologies

As discussed in Chapter IV, ISDN technology has been proposed to improve communication for the R.O.C. Armed Forces. This technology is important not only for analog voice signal transmission, but also because it can provide modern data transmission, teletex, facsimile, videotex, and teleconferencing capabilities. ISDN and other modern integrated digital communication technologies are proposed as part of the framework for the IDCN, based on the unique requirements of the R.O.C. Armed Forces.

ISDNs provide end-to-end digital 64 kbps bit-rate connections between users; no analog signals are used in the link. ISDN brings digital transmission all the way to the user premises using digital subscriber loops that link an ISDN end user terminal to the ISDN exchange. Services dependent on a digital interface, such as data, can be provided directly without an analog-to-digital modem.

ISDN communication services make use of circuit-switching technology, packet-switching technology, and hybrid-switching technology. Circuit switching technology can provide real time voice communication along with integrated services such as video and computer communications. Hybrid switching technology can provide both voice and data signal transmission.

D. U.S. DDN AS A MODEL

The U.S. DDN has been designed to meet DoD requirements for a secure command and control communication network. This common-user world-wide data communications network allows communications that range from the most mundane matters of logistics to critical intelligence data transmitted among mainframe systems at various security levels.

The DDN has successfully provided a cost saving, survivable, secure, reliable, and interoperable network for its users for over a decade. Thus the U.S. DDN model should be considered in the design of the IDCN framework, although the model also should include concepts from modern communication technologies.

E. IDCN FRAMEWORK

1. Local Area Networks

LANs will have a major role in the IDCN, since they allow computers using common protocols to communicate at very high bit rates over a small geographical area. LANs can increase employee productivity and efficiency. They also permit sharing of resources and facilities to reduce the costs of communications.

In general, the distribution of data within an installation such as a military base is best accomplished via a separate telecommunication facility located at that installation. This facility may be a LAN or PBX, and its components can be connected using guided transmission media. These individual LANs then can be connected with the overall IDCN WAN.

Unguided transmission media will be necessary to connect mobile platforms such as naval ships and mobile vehicle units, as shown in Figure 5-4. These interconnected platforms can be considered as LANs. They also can be connected with the IDCN WAN for wide-area communications.

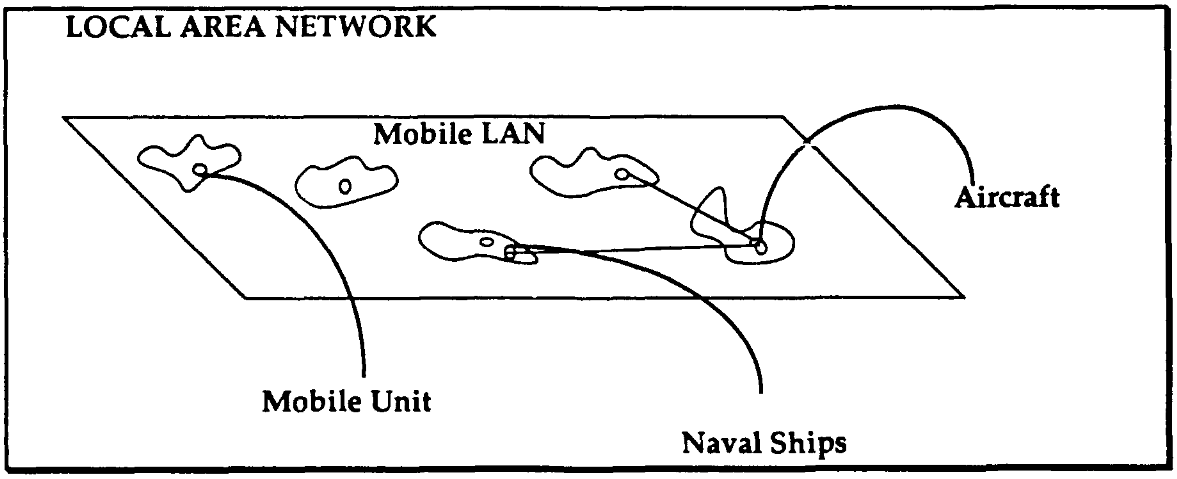

Figure 5-4. Unguided Transmission Media Mobile Platform Network

2. Wide Area Network

A country-wide WAN will be necessary to provide transmission paths among the various individual computers and LANs for military long-haul, unclassified data. The existing commercial R.O.C. WAN illustrated in Figure 5-2 can provide the backbone for the IDCN and its military services. Using encryption techniques, classified data also could be transmitted via the commercial WAN.

Since WANs are used to transmit a variety of signals, the IDCN may require the use of several kinds of transmission media. However, for guided transmissions, optical fiber probably will be the main transmission medium to be used on the islands. The proposed overall structure of the IDCN is shown in Figure 5-5.

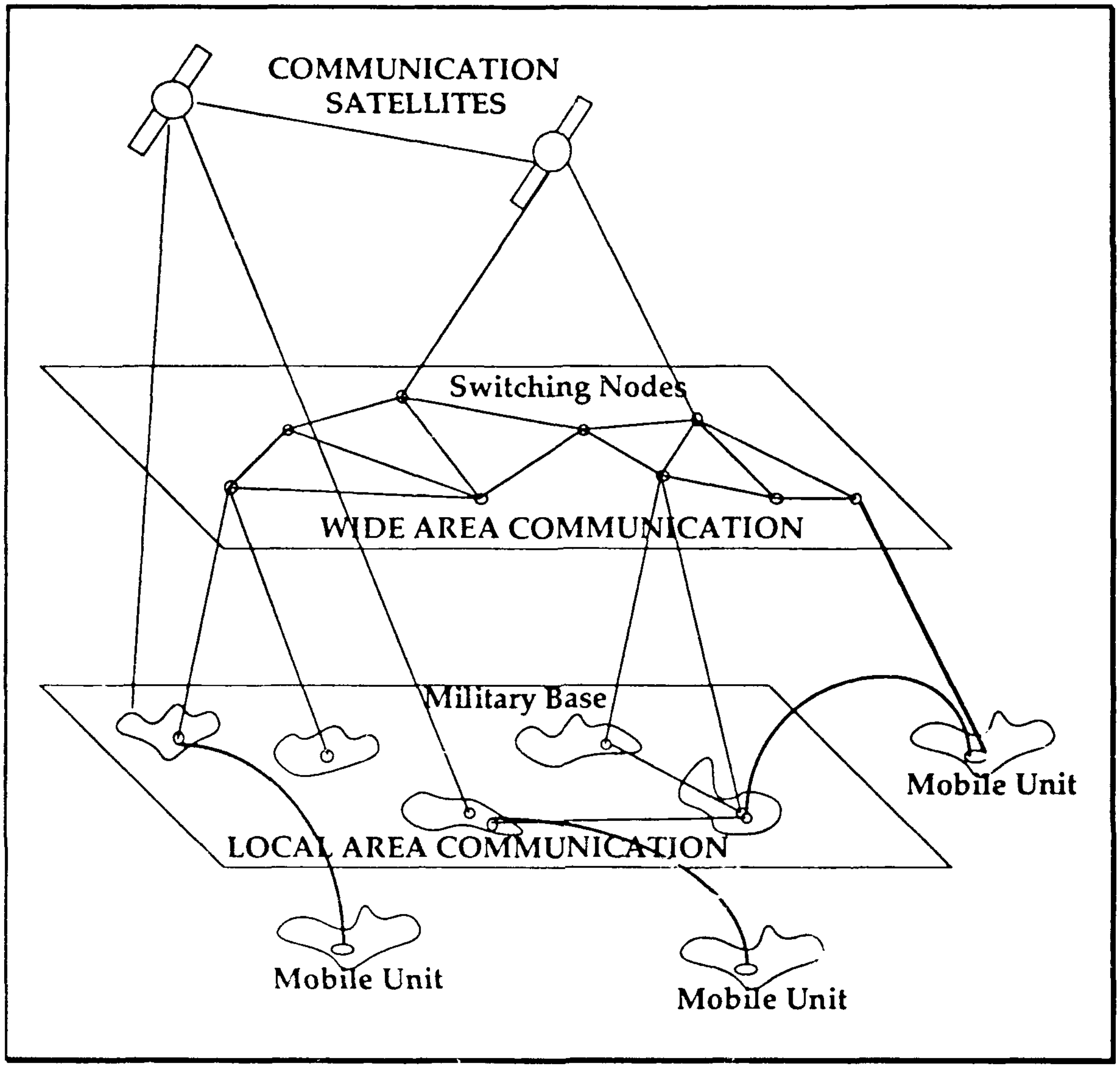

Figure 5-5. Proposed Overall Structure of the IDCN

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

To ensure its continued sovereignty and security, the R.O.C. must maintain strong military forces. It is critical that the R.O.C. Armed Forces have an efficient communication network to support C3I, administration management, logistics supply, and auxiliary tactical communication systems. As discussed in Chapter II, the field of telecommunications has undergone significant changes in the past two decades. Rapid development of new computer and modern digital data communications technologies have had a great influence on both military and commercial telecommunication. These advanced technologies can be used by the R.O.C. to develop a much-needed resource, an Integrated Defense Communication Network.

U.S. DDN technology has significantly improved network communication speed, security, reliability, interoperability, survivability, and cost savings for the U.S. military. The U.S. DDN can be used as a model for a successful military network. This model, combined with concepts from modern communication technology, can be used to develop the conceptual framework for the proposed IDCN for the R.O.C. Armed Forces.

In the long term, ISDN technology is expected to fulfill its promise of support for military C3I system users who need integrated voice, data, and image communications. ISDN appears to offer great potential for solving many of the problem that have plagued C3I systems for years. ISDN digital technology provides inherent cost and performance benefits. ISDN also provides greater network flexibility. This technology also can be used for development of the proposed IDCN. The framework of IDCN provided in Chapter V has combined DDN technology and ISDN standards, and employs modern integrated digital technology to approach its goal.

B. RECOMMENDATIONS

The following recommendations are offered for further consideration by the R.O.C. Armed Forces.

- R.O.C.'s DoD planning activities that are responsible for enhancements to or new acquisitions of C3I systems should utilize ISDN standards.
- R.O.C.'s DoD should consider cooperating with the R.O.C. Department of Transportation to build, share, or lease WAN facilities for military use.
- In order to achieve an optimum communication system, further study should focus on the application of integrated digital communication technology, as discussed in Chapter II, Chapter III, and Chapter IV.
- The general network design plan provided in Chapter V should be considered during development of detailed designs for an IDCN.
- A cost analysis should be conducted to determine the feasibility of network development and the best techniques for network management.
- A detailed network development procedure should be documented prior to starting IDCN development.

REFERENCES

1. *Defense Foreign Affairs Handbook,* Perth Corporation, 19P7.

2. *Worldwide Directory of Defense Authorities,* Lambert Publications, Inc., 1984.

3. Schwartz, M., *Telecommunication Networks: Protocols, Modeling and Analysis,* Addison-Wesley Publishing Company, 1988.

4. Stallings, W., *Data and Computer Communications,* Macmillan Publishing Company, 1988.

5. Black, U., *Data Networks,* Prentice-Hall, Inc., 1982.

6. Stanley, W. D., *Electronic Communications Systems,* Prentice-Hall, Inc., 1982.

7. Lee, E. A., and Messerschmitt, D. G., *Digital Communication,* Kluwer Academic Publishers, 1990.

8. Tanenbaum, A. S., *Computer Networks,* Prentice-Hall, Inc., 1988.

9. Rao, J. R., "An Orientation for Production Quality Networks," *IEEE* , June 1989.

10. Reichard, G. E., "Data Network Platforms and Technologies," *MIDCOM 1989 Conference Record,* 1989.

11. Stanley, W. D., *ISDN: An Introduction,* Prentice-Hall, 1989.

12. Tice, R. M., "Connecting to the DDN Using the DCA's Network Access Component," *IEEE INFOCOM 86 Symposium,* August 1986.

13. Jordan, E. C., *Reference Data for Engineers: Radio, Electronics, Computers, and Communications,* Howard W. Sams & Company, 1989.

14. Fidelman, R. M., Herman, G. J., and Baum, S. M., "Survivability of the Defense Data Network," *Signal,* May 1986.

15. Freeman, R. L., *Telecommunication Transmission Handbook*, John Wiley & Sons, Inc., 1989.

16. Brown, J. K., and Lew, P. M., "Critical User Issues for Fiber Backbones," *Telecommunications*, May 1990.

17. Defense Communications Agency, *Defense Data Network*, 1984.

18. Maybaum, F. L., "Defense Data Network an Overview," *IEEE INFOCOM 86 Symposium*, August 1986.

19. Roberts, J., "The Defense Data Network," *Chips*, January 1987.

20. Defense Communications Agency, *Defense Data Network Program Plan*, June 1982.

21. Powers, M. S., Cheney, P. H., and Crow, G., *Structured Systems Development*, Boyd & Fraser Publishing Company, 1990.

22. Morgan, W. L., and Gordon, G. D., *Communications Satellite Handbook*, John Wiley & Sons, Inc., 1989.

23. Stremler, F. G., *Introduction to Communication Systems*, Addison-Wesley Publishing Company, 1990.

24. Monk, A., *Fundamentals of Human-Computer Interaction*, Academic Press, Inc., 1984.

25. Yourdon, E., *Modern Structured Analysis*, Prentice-Hall, Inc., 1989.

26. Cheng, C. W., and Persson, S. Y., "Technology Transfer," *Electrical Communication*, v. 61, n. 2, 1987.

27. Defense Communication Agency, *The Defense Data Network: High Capacity for DoD Data Transmission*, 1986.

28. Quarterman, J. S., and Hoskins, J. C., "Notable Computer Networks," *Communications of the ACM*, October 1986.

29. Laudon, K. C., and Laudon, J. P., *Management Information Systems*, Macmillan Publishing Company, 1988.

30. Rodriguez, J. M., "A Portable Computer Access Architecture for the DDN," *IEEE INFOCOM 86 Symposium*, August, 1986.

31. Elsam, E. S., "The Defense Data Network Hits Its Stride," *Telecommunications*, May 1986.

32. Boomstein, A., and Tyson, J., "Teleconferencing System Design," in *Electronic Communications Handbook*, A. F. Inglis, ed., McGraw-Hill Book Company, 1988.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Professor Judith H. Lind, Code OR/Li Department of Operation Research Naval Postgraduate School Monterey, CA 93943-5000	2
4.	Professor Dan C. Boger, Code AS/Bo Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943- 5000	2
5.	Naval Academy Library Kaohsiung, Tsoying P.O. Box 90175 Taiwan, Republic of China	2
6.	Yu-Lin Wang, No. 1-7, Lane 17, Wo-Long St, Taipei, Taiwan, Republic of China	5